INCM
Autoridade Reguladora das Comunicações

I RELATÓRIO DE SEGURANÇA NAS TELECOMUNICAÇÕES 2024 - TELEFONIA MÓVEL

RUMO A TRANSFORMAÇÃO DIGITAL

Ficha Técnica:

Título: I Relatório de Segurança nas Telecomunicações 2024 - Telefonia Móvel
Autor: Instituto Nacional das Comunicações de Moçambique – INCM
Ano de Publicação: 2025
Revisão: Ídolo EI
Layout e Paginação: Ídolo EI
Tradução: Ídolo EI

I RELATÓRIO DE SEGURANÇA NAS TELECOMUNICAÇÕES 2024 - TELEFONIA MÓVEL

RUMO A TRANSFORMAÇÃO DIGITAL

Índice

Índice de Figuras

Índice de Tabelas

SUMÁRIO EXECUTIVO

O presente relatório fornece uma visão geral sobre a segurança no sector das telecomunicações em Moçambique, incidindo particularmente nas situações de fraudes, destruição de infra-estruturas e cibersegurança no subsector de telefonia móvel. O documento foi elaborado com base nos relatórios resultantes das actividades de monitoria do tráfego da Autoridade Reguladora das Comunicações (INCM), nas actividades dos operadores de telefonia móvel e nas denúncias submetidas na plataforma denúncias (https://fraude-denuncias.pgr.gov.mz).

Durante o ano de 2024, foram registadas 555.481 (quinhentos e cinquenta e cinco mil quatrocentos e oitenta e uma) ocorrências de fraudes, com destaque para três principais tipologias: SMS-Phishing com 237.716 (duzentos e trinta e sete mil setecentos e dezasseis) casos, correspondendo a 42,8%; Registo Fraudulento de Cartões SIM com 211.278 (duzentos e onze mil duzentos e setenta e oito) casos, perfazendo 38%; e Fraude por SIM-BOX, com 94.385 (noventa e quatro mil trezentos e oitenta e cinco) casos, representando 17%. No conjunto, estas tipologias correspondem a mais de 97% do total das fraudes identificadas.

As fraudes foram detectadas maioritariamente pelos sistemas internos dos operadores (53%) e nas actividades de monitoria do tráfego efectuada pelo INCM (46,9%). A plataforma de denúncias de participação pública, registou apenas 0,1% das ocorrências, o que evidenciou a necessidade de ampliar a sua acessibilidade e confiança junto dos subscritores.

A taxa de sucesso das fraudes foi de 66,3%, sobre um total de 838.154 (oitocentos e trinta e oito mil cento e cinquenta e quatro) tentativas, e a estimativa de incidência é de uma (1) fraude por cada 38 (trinta e oito) subscritores. Em termos geográficos, a província de Nampula registou a maior incidência de fraudes, correspondendo a 45% do total detectado. Segue-se a cidade de Maputo, com 30%, e a província de Maputo, com 12%. No conjunto, estas três regiões concentraram 87% dos casos reportados.

O impacto financeiro global estimado ascende a 63.332.090,00 MT (sessenta e três milhões, trezentos e trinta e dois mil e noventa meticais), o que corresponde a cerca de 1.000.000,00 USD (um milhão de dólares americanos). Destacam-se os prejuízos relacionados com a fraude por exploração de API, no montante de 42.000.000,00 MTN (quarenta e dois milhões de meticais); fraude por SIM-BOX, com 14.000.000,00 MTN (catorze milhões de meticais); registo fraudulento de cartões SIM, com 6.200.000,00 MTN (seis milhões e duzentos mil meticais); e SIM-SWAP, com 950.000,00 MTN (novecentos e cinquenta mil meticais).

Face ao cenário apresentado, durante o ano de 2024 foram tomadas várias medidas com destaque para: o bloqueio de 208.878 (duzentos e oito mil oitocentos e setenta e oito) cartões SIM, a instauração de processos disciplinares e judiciais, a avaliação do nível de maturidade dos operadores e a proposta de estabelecimento de uma Equipa de Resposta a Incidentes de Segurança no sector das Telecomunicações (ERIST).

Adicionalmente, avançou-se com a implementação do Decreto n.º 23/2023, que introduz o registo biométrico dos subscritores, limita o número de cartões SIM por titular e prevê a realização periódica de prova de vida.

Este relatório demonstra que, apesar dos esforços em curso, persistem fragilidades críticas na prevenção, detecção e resposta a fraudes. Torna-se, por conseguinte, imperativo consolidar os mecanismos de controlo, promover a literacia digital dos consumidores e reforçar a articu-

lação entre os operadores, o regulador e o sistema judicial. Estas medidas são essenciais para assegurar a protecção dos interesses dos consumidores, garantir a integridade das redes e fomentar um ambiente de comunicações seguro e confiável em Moçambique.

No que diz respeito aos equipamentos terminais, estima-se a existência de 10.200.000 (dez milhões e duzentos mil) dispositivos não homologados em uso, frequentemente associados a práticas fraudulentas no sector das telecomunicações.

Relativamente à resiliência das infra-estruturas, o país foi afectado por três ciclones tropicais durante o ano de 2024, que comprometeram a disponibilidade das redes e dos serviços, sobretudo na região norte. O impacto financeiro da reposição das infra-estruturas danificadas ascendeu a 10.771.473,60 USD (dez milhões, setecentos e setenta e um mil, quatrocentos e setenta e três dólares americanos e sessenta cêntimos), de acordo com os prejuízos reportados por três operadores de telefonia móvel.

1. INTRODUÇÃO

O Relatório de Fraudes nas Comunicações – 2024 sistematiza as informações recolhidas pela Autoridade Reguladora das Comunicações (INCM), no âmbito das suas actividades de fiscalização e controlo do tráfego, em conformidade com o Regulamento de Segurança de Redes de Telecomunicações e demais instrumentos legais aplicáveis ao sector das comunicações.

O presente relatório tem como propósito apresentar uma análise circunstanciada sobre o estado actual da segurança no sector das telecomunicações em Moçambique, com especial incidência no subsector da telefonia móvel. Nesse contexto, procede-se à identificação das principais ameaças e vulnerabilidades associadas às práticas fraudulentas, aos actos de pirataria e à resiliência das infra-estruturas críticas. A partir dessa análise, são formuladas propostas orientadas para o fortalecimento da resiliência dos activos, dos serviços e dos subscritores.

Actualmente, encontram-se licenciados, no segmento da telefonia móvel, três operadores, designadamente: Tmcel, Vodacom e Movitel, devidamente autorizados a prestar serviços de voz, de transmissão de dados e de mensagens curtas (SMS) a uma população estimada em 33.000.000 (trinta e três milhões) de habitantes. No que concerne à cobertura, os serviços de telefonia móvel abrangem aproximadamente 80% do território nacional, registando-se, no período em análise, um total de 21.000.000 (vinte e um milhões) de subscritores.

Em paralelo, cada um dos operadores dispõe de uma empresa subsidiária autorizada a prestar serviços de moeda electrónica, nomeadamente: Mkesh (Tmcel), M-Pesa (Vodacom) e e-Mola (Movitel), que, em conjunto, servem cerca de 16.000.000 (dezasseis milhões) de subscritores, conforme consta do Resumo Mensal de Informação Estatística do Banco de Moçambique, referente a Janeiro de 2024.

O acelerado crescimento do sector, aliado à massificação do acesso à Internet e à crescente dependência de infra-estruturas digitais, trouxe consigo desafios prementes no domínio da segurança das comunicações, designadamente no combate a fraudes cada vez mais sofisticadas, na protecção dos sistemas contra ameaças cibernéticas e na mitigação dos impactos das alterações climáticas. Cumpre igualmente salientar que, no período em apreço, a ocorrência de fenómenos climáticos extremos, em particular a passagem de três ciclones tropicais, comprometeu de forma significativa a disponibilidade e a continuidade dos serviços de telecomunicações em várias regiões do país.

O cenário actual é caracterizado pela ocorrência de diversas tipologias de fraude, destacando-se o registo fraudulento de cartões SIM, a clonagem de cartões SIM (*SIM swap*), práticas de *phishing* (por SMS e chamadas telefónicas), fraudes nos serviços de moeda electrónica (tais como M-Pesa, e-Mola e Mkesh), bem como o roubo de dados pessoais e bancários. Persistem vulnerabilidades nos mecanismos de identificação de equipamentos terminais, fragilidades na continuidade dos serviços e lacunas na protecção contra ciberataques.

Diante deste panorama, o presente relatório visa apresentar uma avaliação aprofundada da situação vigente, com os seguintes objectivos específicos: mapear o panorama nacional das fraudes no sector da telefonia móvel; identificar as principais ameaças à segurança das comunicações; catalogar as tipologias de fraude mais prevalentes; cartografar os locais de ocorrência e as respectivas fontes de reporte; avaliar o impacto económico, social e operacional das fraudes; propor medidas de mitigação sustentáveis; e analisar os impactos decorrentes dos fenómenos climáticos extremos sobre as infra-estruturas de telecomunicações.

São, por fim, formuladas recomendações estratégicas para o reforço da resiliência das redes e da segurança dos consumidores, no contexto da transformação digital, exigindo respostas coordenadas de todos os actores do sector.

2
CONTEXTO GLOBAL

2. CONTEXTO GLOBAL

A Análise Global da Segurança das Comunicações em 2024, elaborada com base em relatórios da GSMA (Global System for Mobile Communications Association), da UIT (União Internacional das Telecomunicações) e da Data Reportal, revela um cenário em constante evolução, caracterizado por avanços tecnológicos, desafios crescentes no domínio da Cibersegurança e regulamentações sujeitas a actualizações permanentes.

2.1. Estatística Global dos Subscritores de Telecomunicações

A figura abaixo, extraída do portal Data Reportal, apresenta o panorama geral dos subscritores de serviços de telecomunicações em 2024, relativamente ao número total da população, ao número de subscritores de serviços de telecomunicações, aos subscritores com acesso à Internet e aos utilizadores activos das redes sociais.

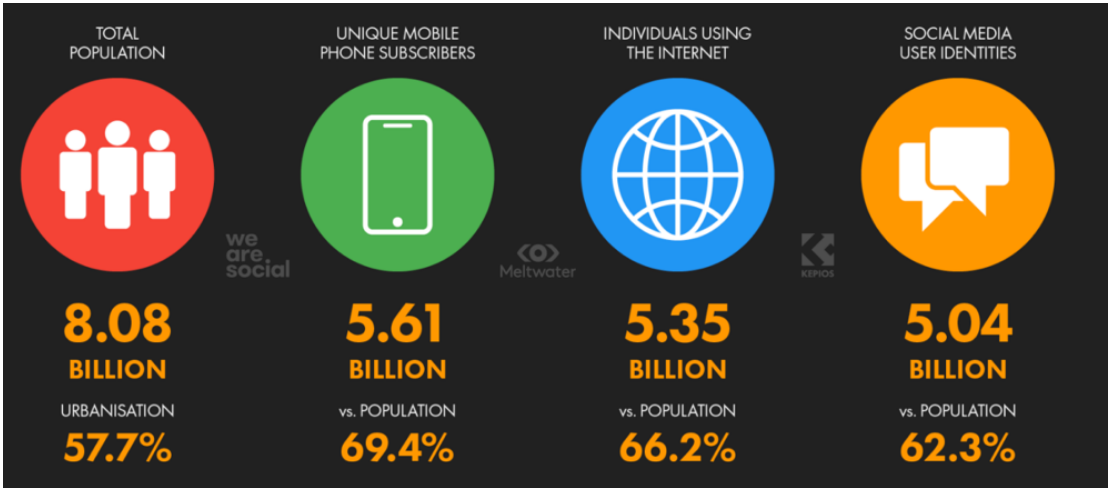


Figura 1 - Panorama Geral das Comunicações 2024
Fonte: https://www.DataReportal.com

2.2. Principais Ameaças Globais a Subscritores de Telecomunicações

O relatório GSMA Mobile Telecommunications Security Landscape 2024 destaca as principais ameaças ao sector das telecomunicações, entre as quais salientam-se os ataques dirigidos às operadoras, as vulnerabilidades nas redes 5G, IoT e computação em nuvem, bem como fraudes sofisticadas e novas ameaças potenciadas pela inteligência artificial.

Segundo a tabela abaixo, os dados globais reportados indicam uma prevalência significativa de diversos tipos de fraudes no sector das telecomunicações e dos serviços financeiros móveis.

Tendência	Casos	Fonte
Registo Fraudulento de cartões SIM	90,38% de prevalência entre operadores	GSMA Fraud Typologies Report 2024
SIM-BOX (Fraude de Alta Complexidade)	3,11 Biliões	CFCA Fraud Loss Survey 2021
VOICE-Phishing	Dados não especificados	GSMA State of the Industry Report 2023
Mobile Money	1 bilião em perdas em África	
Engenharia Social	88,46% de prevalência entre operadores	GSMA Fraud Typologies Report 2024
Internal Fraud	86,54% de prevalência entre operadores	GSMA Fraud Typologies Report 2024
Fraude por SIM Swap	78,85% de prevalência entre operadores	GSMA Fraud Typologies Report 2024
Fraude Cibernética	59,62% de prevalência entre operadores	GSMA Fraud Typologies Report 2024
Fraude por Comissões (Agentes)	55,77% de prevalência entre operadores	GSMA Fraud Typologies Report 2024

Tabela 1 - Principais ameaças globais a subscritores de telecomunicações

Com base nas tendências observadas e na frequência com que afectam os operadores a nível internacional, destacando-se:

- SMS-Phishing (Smishing) – estima-se que ocorram entre 300.000 e 400.000 ataques diários a nível mundial, representando uma ameaça persistente e crescente à segurança dos utilizadores móveis;
- Registo Fraudulento de Cartões SIM – apresenta uma elevada incidência, afectando aproximadamente 90,38% dos operadores de telecomunicações;
- SIM-BOX (Fraude de Alta Complexidade) – afectou aproximadamente 3,11 biliões de consumidores;
- Fraude em Mobile Money – registou-se perdas superiores a 1.000.000,00 USD (um milhão de dólares americanos) apenas no continente africano;
- Engenharia Social – estima-se que 88,46% dos operadores tenham sido afectados por casos de engenharia social, segundo dados da GSMA. Este tipo de fraude caracteriza-se pela manipulação psicológica de indivíduos, com o objectivo de obter informações sensíveis ou acesso não autorizado a sistemas e recursos;
- Fraude Interna (Internal Fraud) – afecta 86,54% dos operadores de telecomunicações;
- Fraude por SIM Swap – afecta 78,85% dos operadores, representa um risco crescente para a segurança dos subscritores, sobretudo no acesso a contas bancárias e serviços sensíveis;
- Fraude Cibernética – afecta 59,62% dos operadores a nível global;
- Fraude por Comissões (Agentes de Mobile Money) – afecta 55,77% dos operadores.

2.3. Principais Ameaças a Redes Móveis

O ambiente das redes móveis apresenta actualmente um cenário de ameaças cada vez mais sofisticado e diversificado. O aumento da virtualização, a crescente dependência de infra-estruturas complexas e a constante evolução das tecnologias de comunicação expõem os sistemas a novos métodos de ataque, comprometendo a segurança e a privacidade dos subscritores e operadores.

A tabela abaixo sintetiza os principais desafios identificados no relatório anual da GSMA – *Mobile Telecommunications Security Landscape* 2024, agrupando as ameaças mais relevantes — desde ataques a infra-estruturas virtualizadas e operadoras móveis até riscos emergentes, como os ataques a protocolos de sinalização e a proliferação de spyware. Esta secção descreve e analisa, de forma pormenorizada, cada uma dessas ameaças, sublinhando a necessidade de adoptar abordagens de defesa dinâmicas e permanentemente actualizadas.

Categoria de Risco	Descrição
Ataques a Operadoras	Incluem tentativas de acesso não autorizado a sistemas e dados das operadoras, visando comprometer a integridade e a disponibilidade dos serviços de telecomunicações.
Infraestrutura Virtualizada e 5G	A migração para infraestruturas baseadas em nuvem e a implementação do 5G introduzem novas vulnerabilidades, exigindo medidas de segurança robustas para proteger os elementos virtualizados da rede.
Cadeia de Suprimentos	Riscos associados à dependência de múltiplos fornecedores para hardware e software, onde vulnerabilidades em qualquer ponto da cadeia podem comprometer a segurança da rede.
Abuso de Títulos Globais e Interconexão	Exploração de protocolos de sinalização, como o SS7, para interceptar comunicações, obter informações de localização ou realizar fraudes, afectando a confiança nas interconexões entre redes.
Malware e Ransomware	Aumento de ataques que utilizam software malicioso para comprometer dispositivos e redes, com o objectivo de extorquir valores ou causar interrupções nos serviços.
Spyware Comercial	Utilização de software espião para monitorar e colectar informações confidenciais dos usuários, representando uma ameaça à privacidade e à segurança dos dados pessoais.
Segurança de Aplicações Móveis	Riscos decorrentes de vulnerabilidades em aplicações móveis, que podem ser exploradas para acesso não autorizado a dados ou funcionalidades dos dispositivos dos usuários.
Novos e Reempacotados Tipos de Fraude	Evolução contínua das técnicas de fraude, onde métodos antigos são adaptados ou combinados com novas abordagens para enganar usuários e sistemas de segurança.
Engenharia Social e Phishing	Tácticas que exploram a confiança dos usuários para obter informações sensíveis ou acesso a sistemas, incluindo SMS-Phishing e Voice-Phishing.
Inteligência Artificial Generativa	Uso de IA para automatizar e aprimorar ataques cibernéticos, criando desafios adicionais para a detecção e mitigação de ameaças, além de levantar questões éticas e de governança de dados.
Interrupções por Factores Externos	Eventos como sabotagens, desastres naturais ou decisões políticas que resultam em apagões de internet, afectando a disponibilidade e a resiliência das redes de telecomunicações.

Tabela 2 - Principais Ameaças a Redes Móveis
Fonte: GSMA - Fraud Typologies Report 2024

A figura abaixo apresenta os principais tópicos identificados no relatório anual, organizados em um diagrama que destaca as ameaças e desafios de segurança enfrentados pela indústria móvel. Abaixo está a descrição detalhada.

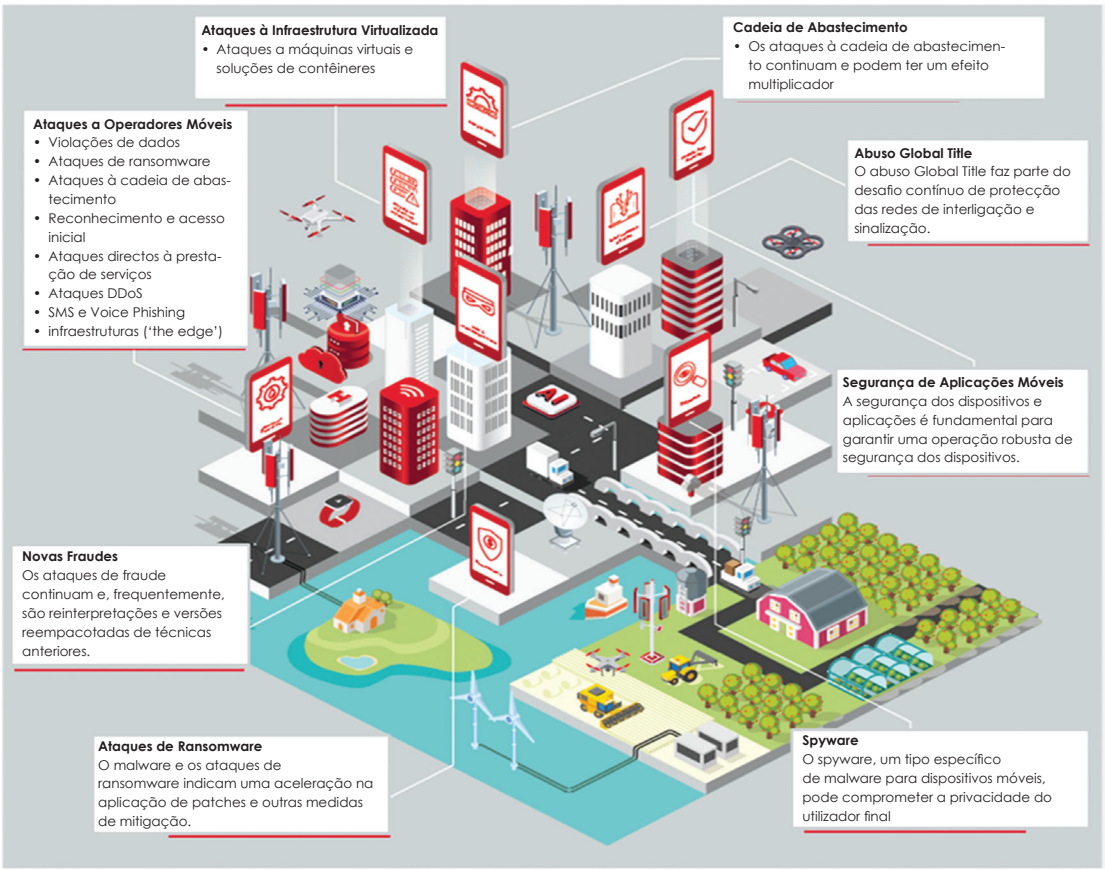


Figura 2 - Principais Ameaças à Redes Móveis

Descrição do Diagrama das Principais Ameaças á Redes Móveis

1. Ataques à Infraestruturas Virtualizadas

- Descrição: incidem sobre máquinas virtuais e soluções baseadas em *contêineres* como (*Docker e Kubernetes*).
- Explicação: A virtualização e a computação em nuvem constituem alvos críticos devido à sua ampla utilização. Ataques bem-sucedidos podem comprometer múltiplos serviços simultaneamente, gerando impactos de grande escala.

2. Ataques à Operadoras Móveis

- Vazamento de dados *(Data breaches)*: Roubo de informações sensíveis dos subscritores ou empresas;
- Ataques de *ransomware*: Criptografia de dados, seguida de pedidos de resgate;
- Ataques à cadeia de fornecimento (*Supply chain attacks*): Exploração de vulnerabilidades em fornecedores terceirizados;
- Ataques directos à prestação de serviços: Interrupção de serviços essenciais (ex.: redes 5G);
- Ataques de DDoS: Sobrecarga dos sistemas, tornando-os inacessíveis;
- Engenharia social: Manipulação de pessoas para obtenção de acesso não autorizado;
- Comprometimento da borda (*'the edge'*): Ataques a dispositivos de borda, como IoT e torres de comunicações.
- Explicação: Estes ataques exploram vulnerabilidades técnicas e humanas, exigindo estratégias de defesa multifacetadas.

3. 3. Fraudes Ré-empacotadas (*New & Re-packaged Fraud*)

- Descrição: Métodos de fraude antigos adaptados a novos contextos.
- Explicação: Criminosos reutilizam técnicas já conhecidas, introduzindo pequenas variações para contornar os sistemas de detecção, o que impõe a necessidade de actualização contínua das defesas.

4. Ataques de *Ransomware*

- Descrição: Reforço da necessidade de aceleração de processos de correcção (*patching*) e mitigação.
- Explicação: O ransomware continua a constituir uma ameaça persistente, exigindo respostas rápidas para limitar os danos causados.

5. Ameaças à Cadeia de Fornecimento (*Supply Chain*)

- Descrição: Ataques que afectam vários elos da cadeia de fornecimento.

- Explicação: A exploração de um único ponto vulnerável pode amplificar consideravelmente o impacto, comprometendo diversas entidades simultaneamente (por exemplo, através do ataque a um fornecedor de *software* utilizado por múltiplas operadoras).

6. Abuso de Título Global (*Global Title Abuse*)

- Descrição: Ameaça dirigida a redes de interconexão e sinalização (tais como SS7 e Diameter).
- Explicação: Consiste na exploração de falhas nos protocolos de sinalização para interceptar chamadas, localizar utilizadores ou desviar tráfego.

7. Segurança de Aplicativos Móveis (*Mobile App Security*)

- Descrição: Realce para a importância da protecção dos dispositivos e aplicações móveis.
- Explicação: Aplicações vulneráveis ou maliciosas podem comprometer tanto a segurança dos utilizadores quanto a integridade das redes.

8. Spyware

- Descrição: *Malware* concebido para violar a privacidade dos utilizadores (ex.: Pegasus).
- Explicação: Para além do roubo de dados, pode ser utilizado para fins de vigilância dirigida, o que exige mecanismos avançados de protecção dos dispositivos.

2.4. Estatísticas Globais de Ataques a Redes de Telecomunicações

Em 2024, o sector das telecomunicações enfrentou uma intensificação sem precedentes das ameaças cibernéticas, com impacto cada vez mais acentuado tanto ao nível financeiro quanto operacional. Os ataques de *ransomware* registaram um aumento em 35% relativamente ao ano de 2023, com perdas médias por incidente estimadas em 4.500.000,00 USD (quatro milhões e quinhentos mil dólares americanos), destacando-se o caso da *Dish Network,* que sofreu cinco dias de interrupção dos serviços e prejuízos avaliados em 100.000.000,00 USD (cem milhões de dólares americanos).

Os ataques de negação de serviço distribuído (DDoS) mantiveram-se como uma ameaça relevante, em termos de incidentes registados em 2023, na ordem de 7.900.000 (sete milhões e novecentos mil). Os custos, por hora, de inactividade variaram entre 50.000,00 USD (cinquenta mil dólares americanos) e 500.000,00 USD (quinhentos mil dólares americanos), sendo o sector das telecomunicações o mais visado, concentrando 28% do total de ataques.

As redes 5G e os ambientes de computação em nuvem continuam a apresentar vulnerabilidades estruturais críticas. Cerca de 60% das falhas reportadas em redes 5G estiveram associadas a *containers* e processos de virtualização, com um tempo médio de correcção de cento e dois (102) dias. Em paralelo, 42% das violações de segurança ocorreram através da exploração de interfaces de programação de aplicações (API).

No domínio das fraudes, salientam-se perdas estimadas em 3.200.000,00 USD (três mil e du-

zentos milhões de dólares americanos) provocadas por tráfego artificial (*AIT – Artificially Inflated Traffic*), e uma elevada incidência de ataques do tipo *smishing*, que afectaram 62% dos utilizadores de serviços móveis.

Adicionalmente, os dispositivos de Internet das Coisas (IoT) tornaram-se alvos prioritários de *malware*, com 1.500.000 (um milhão e quinhentos) de dispositivos comprometidos por *botnets* e um em cada cinco aplicativos móveis contendo software malicioso.

No que respeita à segurança das infra-estruturas de sinalização, 89% das redes SS7 analisadas apresentaram vulnerabilidades críticas, tendo-se verificado que pelo menos 120 operadoras foram afectadas por abusos do protocolo GT (GSM-Terrestrial).

No total, estima-se que as perdas globais associadas à cibercriminalidade no sector das telecomunicações tenham atingido 12.000.000.000,00 USD (doze biliões de dólares americanos) em 2024, com um tempo médio de recuperação por incidente de dezoito (18) dias.

A tabela abaixo apresenta os dados detalhados, acompanhados do respectivo impacto operacional e financeiro.

Categoria de Ataque	Métrica	Valor	Fonte	Impacto Financeiro/Operacional
Ransomware	Aumento anual de ataques	+35% (2023-2024)	GSMA 2024	Custo médio por ataque: $4,5 milhões
Ataques DDoS	Exemplo: Dish Network (2023)	5 dias de downtime	IBM X-Force	Perdas: $100 milhões
	Total global (2023)	7,9 milhões de ataques	Cloudflare	Custo: 50K–50K–500K/ hora (downtime)
	Setor mais atingido	28% dos ataques	Imperva	Maior ataque: 1,1 Tbps
Vulnerabilidades 5G/Cloud	Falhas em containers/ virtualização	60% das brechas em redes 5G	GSMA	Tempo médio para correção: 102 dias
	Ataques a APIs	42% das violações	Salt Security	
Fraudes (AIT, Smishing)	Perdas globais por AIT	$3,2 biliões (2023)	MEF	
	Vítimas de smishing	62% dos usuários	Zimperium	
Spyware/Malware	Dispositivos IoT comprometidos (botnets)	1,5 milhões (2023)	FortiGuard	
	Apps maliciosos (sideloaded)	1 em cada 5	Nokia Threat Intelligence	
SS7/Diameter/ GT Abuse	Redes com falhas críticas em SS7	89%	Positive Technologies	
	Operadoras afectadas por GT Abuse	120 (2023)	GSMA T-ISAC	
Impacto Económico Total	Perdas globais (2024)	$12 biliões	ITU	Tempo médio de recuperação: 18 dias

Tabela 3 - Relação Global de Impacto financeiro e operacional

3 CONTEXTO NACIONAL

3. CONTEXTO NACIONAL

Moçambique, com uma população estimada em cerca de 34.000.000 (trinta e quatro milhões) de habitantes, segundo projecções do Instituto Nacional de Estatística (INE) para 2024, tem registado progressos significativos na expansão do sector das telecomunicações, impulsionados por políticas públicas de inclusão digital, investimentos privados e inovações tecnológicas. Este sector assume-se como um pilar estratégico para o desenvolvimento económico e social do país, ao facilitar o acesso à informação, promover a prestação de serviços públicos e dinamizar os mercados digitais.

Actualmente, o sector de telefonia móvel está licenciado para três operadores nacionais (Vodacom, Movitel e Tmcel) que oferecem serviços de voz, SMS, dados móveis e serviços financeiros móveis, através das suas subsidiárias MPESA, E-MOLA e MKESH, respectivamente.

De acordo com o mais recente Relatório de Regulação do INCM, até ao final de 2023, Moçambique registava aproximadamente 21.000.000 (vinte e um milhões) de subscritores activos de serviços móveis, representando cerca de 64% da população e correspondendo a uma taxa de penetração estimada em 70%. No que concerne aos serviços de acesso à Internet móvel, estima-se que cerca de 8.000.000 (oito milhões) de subscritores aderiram a este serviço, o que equivale a 23% do total de subscritores de telefonia móvel.

Relativamente aos serviços de carteira móvel, apurou-se um total de aproximadamente 16.000.000 (dezasseis milhões) de subscritores, de acordo com o Resumo Mensal de Informação Estatística do Banco de Moçambique, referente a Janeiro de 2024, representando uma taxa de penetração de cerca de 76% entre os subscritores de serviços móveis.

No que concerne à cobertura da rede dos serviços de telefonia móvel, estima-se uma taxa de penetração de cerca de 70% em todo o território nacional, assegurada pelas tecnologias 2G, 3G, 4G e, em algumas regiões, pela tecnologia 5G.

De acordo com dados estatísticos da Statcounter GlobalStats, no período em análise estima-se que se encontrem em circulação cerca de 34.000.000 (trinta e quatro milhões) de terminais móveis activos nas redes de telecomunicações em Moçambique. Deste universo, 23.800.000 (vinte e três milhões e oitocentos mil) correspondem a equipamentos homologados, representando 70% do total, enquanto cerca de 10.200.000 (dez milhões e duzentos mil) são não homologados, equivalentes a 30%.

Segundo o relatório da DataReportal de 2024, até Janeiro de 2024, estimava-se que Moçambique contava com 3.200.000 (três milhões e duzentos mil) utilizadores activos de redes sociais, correspondendo a aproximadamente 9,3% da população total. Este número reflectiu um crescimento significativo de 39,1% face ao ano anterior, o que representa mais 900.000 (novecentos mil) utilizadores.

Entre as plataformas mais populares, o Facebook liderava, com cerca de 3.900.000 (três milhões e novicentos mil) utilizadores em Dezembro de 2024, representando 10,6% da população total. Outras redes sociais, como o Instagram, registavam aproximadamente 637.000 (seiscentos e trinta e sete mil) utilizadores no mesmo período

Apesar dos avanços alcançados, o sector das comunicações continua a enfrentar riscos crescentes em matérias de cibersegurança, impulsionados pela intensificação da digitalização dos serviços, pelo aumento das fraudes electrónicas e pela utilização massiva de plataformas móveis para transacções financeiras.

Adicionalmente, a localização geográfica de Moçambique, na orla do Oceano Índico, expõe o país a fenómenos climáticos recorrentes, em particular os ciclones, que afectam de forma significativa a resiliência e a disponibilidade das infra-estruturas de comunicações. Em 2024, o país foi atingido por três ciclones, os quais impactaram negativamente a continuidade dos serviços de telecomunicações.

As imagens abaixo representam o diagrama do contexto nacional, abrangendo a rede de telecomunicações, utilizadores, equipamentos terminais e utilizadores das redes sociais.

Figura 3 - Contexto das Telecomunicações

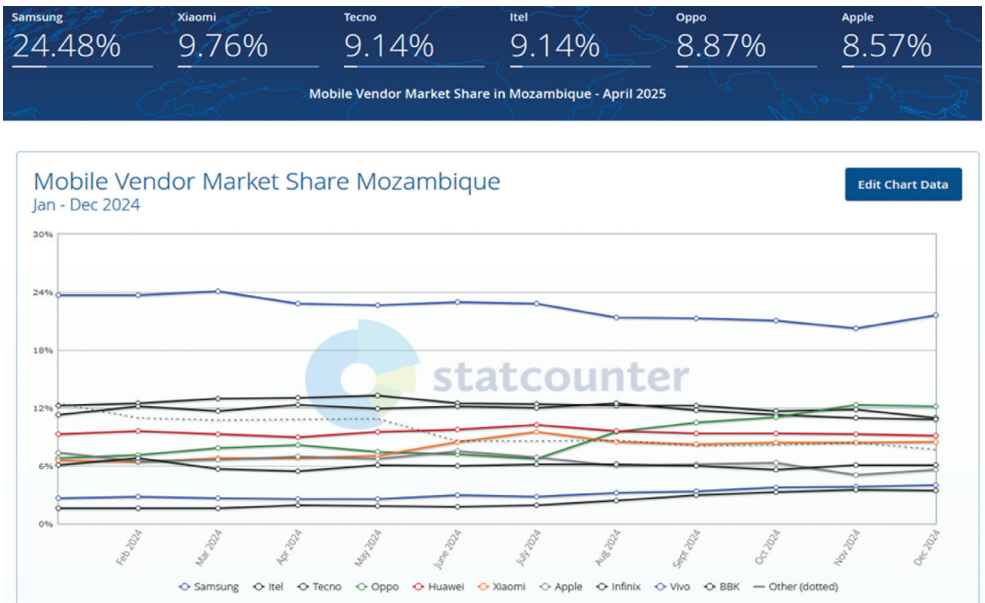


Figura 4 - Estatística de Terminais em Moçambique
Fonte: StatCounter Global Stats

3.1. Classificação de Moçambique na ITU Sobre o Nível de Cibersegurnça

Na edição de 2024 do Índice Global de Segurança Cibernética (GCI), publicado pela União Internacional das Telecomunicações (ITU), Moçambique registou um avanço significativo, passando de 24,19 pontos na edição anterior para 66,05 pontos, representando um aumento de 41,86 pontos. Este progresso é reflexo do empenho do país em fortalecer a segurança cibernética por meio de diversas iniciativas e políticas públicas.

No contexto global, Moçambique ocupa a 123ª posição entre os 194 países avaliados, situando-se no Nível 3 do GCI, que indica um compromisso moderado com a segurança cibernética.

Estes resultados evidenciam o progresso de Moçambique na implementação de políticas e práticas de segurança cibernética, embora persistam desafios a superar, especialmente no âmbito do desenvolvimento de capacidades. O país prossegue os esforços para melhorar a sua posição no GCI, com enfoque na implementação de medidas legais, técnicas e organizacionais, bem como no reforço do desenvolvimento de capacidades e cooperação internacional.

A seguir apresenta-se a tabela com a pontuação obtida por Moçambique nos pilares avaliados pelo Índice Global de Segurança Cibernética (GCI) da União Internacional das Telecomunicações (ITU), acompanhada da imagem com a classificação do país, extraída do Relatório da 5.ª Edição do GCI.

Pilar	Pontuação	Análise
Cooperação	16,58	Destaque: Forte participação em colaborações internacionais.
Medidas Organizacionais	15,75	Sólido: Estratégias e organismos nacionais bem estabelecidos.
Medidas Legais	13,2	Intermediário: Leis existentes, mas com espaço para melhorias.
Medidas Técnicas	11,8	Intermediário: Infraestrutura presente, mas necessita modernização.
Desenvolvimento de Capacidades	7,93	Desafio: Baixo investimento em treinamento e educação em cibersegurança.

Tabela 4 Classificação de Moçambique no Índice de Cibersegurança da ITU
Fonte https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Mozambique

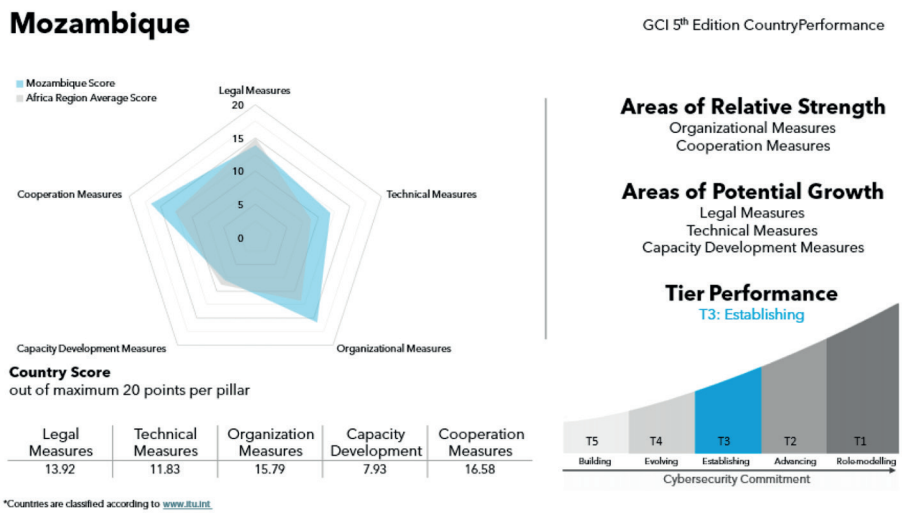


Figura 5 - Imagem Ilustrativa de Posicionamento de Moçambique nos Índices da ITU
Fonte Índice de Global de Cibersegurança da ITU

3.2. Quadro Legal

O combate às fraudes no sector das telecomunicações, aliado ao reforço da segurança e resiliência das redes, assenta num conjunto de instrumentos legais e regulamentares que visam estabelecer um ambiente normativo robusto, capaz de prevenir, detectar e sancionar práticas ilícitas, além de assegurar a resiliência das infra-estruturas críticas de comunicações.

Entre os principais regulamentos que sustentam a actuação neste domínio de segurança cibernética, no país em geral e no sector das comunicações em particular, destacam-se os indicados na tabela abaixo.

Instrumento Legal / Regulamentar	BREVE DESCRIÇÃO
Lei das Telecomunicações (Lei n.º 4/2016, de 25 de Maio)	Estabelece os princípios e regras gerais que regem o sector das telecomunicações em Moçambique, incluindo disposições sobre licenciamento, direitos e deveres dos operadores, protecção dos consumidores e deveres em matéria de segurança das redes.
Lei dAS Transacções Electrónicas (Lei n.º 3/2017, de 9 de Janeiro)	Define os princípios jurídicos aplicáveis às transacções electrónicas e à segurança da informação, incluindo o uso de meios digitais em contextos comerciais e administrativos.
Regulamento de Segurança de Redes de Telecomunicações (Decreto n.º 66/2019, de 1 de Agosto)	Estabelece normas e requisitos mínimos para garantir a disponibilidade, integridade, confidencialidade e autenticidade das redes e serviços de telecomunicações, bem como a protecção de dados dos utilizadores e a resiliência das infra-estruturas de rede.
Regulamento de Controlo de Tráfego de Telecomunicações (Decreto n.º 38/2023, de 3 de Julho)	Define os mecanismos e procedimentos de controlo do tráfego nas redes dos operadores de serviços de telecomunicações, visando garantir maior segurança nos serviços, proteger os interesses dos operadores e do Estado, mitigar fraudes e assegurar a qualidade dos serviços.
Regulamento de Protecção do Consumidor do Serviço de Telecomunicações (Decreto n.º 44/2019, de 22 de Maio)	Estabelece os mecanismos de protecção dos consumidores no mercado das telecomunicações, aplicando-se aos operadores de televisão, telefonia, dados, vídeo e outros que prestam serviços de telecomunicações de uso público, bem como aos consumidores.
Normas Complementares e Circulares Técnicas emitidas pelo Regulador (INCM)	O regulador tem vindo a emitir directivas específicas no âmbito da segurança das redes, protecção de dados dos consumidores, procedimentos de resposta a incidentes e partilha de informação entre os operadores.

Tabela 5 Quadro Legal para Combate a Fraudes

3.3. Análise de Incidentes com Impacto na Segurança e Resiliência das Telecomunicações

A presente secção fornece uma visão geral das principais ocorrências, no ano de 2024, afectaram a segurança e a resiliência das telecomunicações em Moçambique, gerando impactos significativos na estabilidade, na continuidade e na confiança nos serviços de comunicação.

Durante o período em análise, registaram-se diversos eventos adversos, entre os quais destacam-se:

3.3.1. Fraudes em Telecomunicações

No decurso do ano de 2024, registaram-se diversas ocorrências de fraude no sector das telecomunicações, abrangendo, entre outras práticas ilícitas, burlas realizadas através de chamadas telefónicas e mensagens fraudulentas, o registo indevido de cartões SIM, bem como a manipulação irregular de serviços de valor acrescentado. Estes incidentes provocaram prejuízos financeiros tanto para os subscritores quanto para os operadores, comprometendo, adicionalmente, a confiança na utilização dos serviços de comunicação.

A dinâmica mais recorrente dos esquemas fraudulentos é ilustrada na figura seguinte, que

sintetiza o seu grau de complexidade. De modo geral, as fraudes têm início com o registo fraudulento de cartões SIM, posteriormente inseridos em terminais não homologados ou com códigos IMEI adulterados. Após a autenticação na rede de telecomunicações, os defraudadores passam a aceder aos serviços com identidade anónima, desencadeando assim, diversas modalidades de fraude descritas neste relatório.

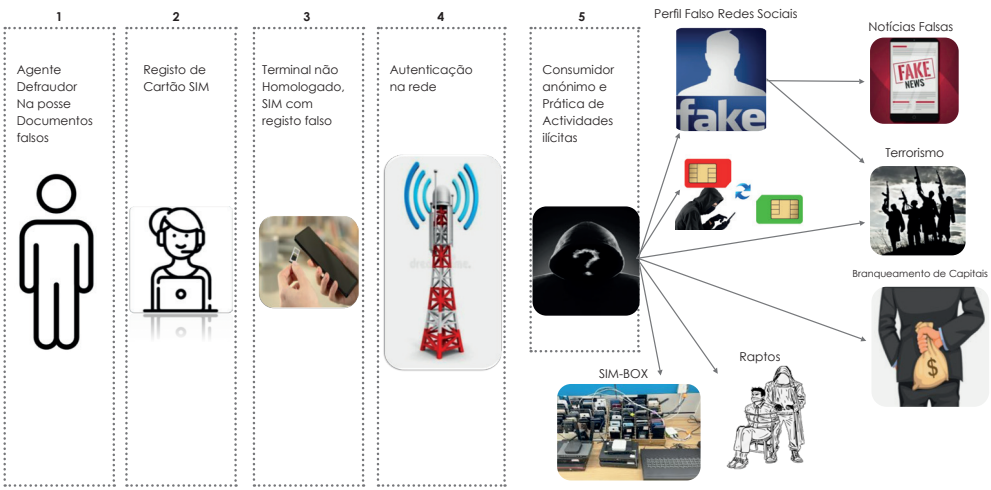


Figura 6 - Fluxo de Ocorrência de Fraudes em Telecomunicações
Fonte INCM

No decurso do ano de 2024, e com base na consolidação de dados provenientes de diversas fontes de reporte de incidentes a nível nacional nomeadamente os operadores de telecomunicações, a Plataforma de Denúncia de Fraudes e a Plataforma de Controlo de Tráfego gerida pela Autoridade Reguladora, foi possível identificar **851.154 (oitocentos e cinquenta e um mil, cento e cinquenta e quatro.)** tentativa de fraudes, das quais **558.448 (quinhentos e cinquenta e oito mil quatrocentos e quarenta e oito)** foram confirmadas com sucesso.

De acordo com os dados analisados, destacam-se três tipologias de fraude com maior incidência:

- SMS-*Phishing*, com 42,8% do total de casos;
- Registo Fraudulento de Cartões SIM, com 38 %; e
- Fraude por *SIM-Box*, com 17 %.

Estas três categorias representam, no seu conjunto, mais de 97% do total de fraudes registadas, evidenciando um padrão de ataque centrado na manipulação de utilizadores e na exploração de falhas nos sistemas de activação e encaminhamento de chamadas.

As restantes tipologias, embora com menor expressão percentual, assumem relevância estratégica por evidenciarem vulnerabilidades específicas do ecossistema digital e operacional.

Destacam-se, entre estas, o *SIM-Swap*, a exploração de *API Bundle* e as fraudes internas, que, apesar de residuais em volume, representam riscos críticos para a integridade dos sistemas e para a confiança dos utilizadores.

A tabela seguinte apresenta a distribuição percentual das principais categorias de fraudes identificadas no território nacional durante o período em análise:

Tipologia de Fraude	Casos	PER (%)	Características
SMS-Phishing	237.716	42,80%	Mensagens fraudulentas para obtenção de dados pessoais
Registo Fraudulento	211.278	38,00%	Activação ilegal de linhas ou serviços
SIM-BOX	94.385	17,00%	Desvio de tráfego internacional através de gateways ilegais
Engenharia Social	9.501	1,70%	Manipulação psicológica de vítimas
VOICE-Phishing	1.200	0,20%	Chamadas fraudulentas para obtenção de informações
WANGIRI IRSF	593	0,10%	Chamadas perdidas para números premium
SIM-SWAP	530	0,10%	Clonagem de números para acesso a contas
Mobile Money	158	0,03%	Fraudes em transações financeiras móveis
API Boundle	102	0,02%	Exploração de vulnerabilidades em APIs
Internal Fraud	16	0,00%	Fraudes cometidas por colaboradores
Ataque Cibernético	2	0,00%	Tentativas de invasão a sistemas
Total	555 481	100%	---

Tabela 6 - Visão Geral das Fraudes em 2024
Fonte INCM

3.3.2. Pirataria e Interferências Ilegais

Em 2024, registaram-se casos de pirataria que comprometeram a segurança e a qualidade das telecomunicações, envolvendo a transmissão não autorizada de sinais de radiodifusão, a utilização indevida de frequências e a importação de terminais não homologados com códigos IMEI adulterados. Estas práticas provocaram interferências nas redes de comunicação e afectaram serviços críticos, como as comunicações aeronáuticas. Como consequência, três rádios comunitárias na província de Nampula foram forçadas a suspender temporariamente as suas emissões, de modo a salvaguardar a segurança das operações aéreas.

3.3.3. Eventos Naturais – Ciclones Tropicais

Em 2024, fenómenos climáticos extremos, em particular ciclones tropicais, causaram danos significativos nas infra-estruturas de telecomunicações, afectando torres de transmissão e redes eléctricas, o que resultou em interrupções prolongadas nos serviços de voz e dados, com impacto crítico nas zonas mais vulneráveis.

4
SITUAÇÃO DAS FRAUDES NO SECTOR DAS TELECOMUNICAÇÕES

4. Situação das Fraudes no Sector das Telecomunicações

4.1. Fonte de Dados Sobre Fraudes

A análise das fraudes apresentada neste relatório assenta, em dados recolhidos a partir de três fontes fundamentais, que constituem os principais canais e sistemas através dos quais são identificadas, registadas e reportadas actividades fraudulentas no sector das telecomunicações. Estas fontes desempenham um papel crucial na detecção, análise e mitigação de fraudes, assegurando uma resposta célere e eficaz. São elas:

- **Regulador:** através dos canais de atendimento aos utentes, incluindo a linha do utente, bem como dos mecanismos adoptados no processo de monitoria e fiscalização das actividades dos operadores, permitindo a recolha de informações sistematizadas sobre padrões de tráfego anómalos;
- **Operadores de Telecomunicações:** mediante a disponibilização regular de dados e informações sobre incidentes, fraudes e denúncias, que detectem directamente, quer lhes sejam reportados pelos subscritores; e
- **Plataforma de Denúncias:** canal online disponibilizado ao público, que permite aos consumidores reportar ocorrências suspeitas ou confirmadas de fraude através de uma interface web acessível.

Estas fontes possibilitam a obteção de uma visão abrangente e actualizada do panorama das fraudes no sector da telefonia móvel, permitindo identificar padrões recorrentes, zonas geográficas de maior incidência e fragilidades nos mecanismos de prevenção e resposta existentes.

4.1.1. Actuação do Regulador

Uma das componentes essenciais do processo de monitoria e fiscalização conduzido pelo Regulador reside na capacidade de detectar situações suspeitas de fraude. Neste âmbito, foi identificado um total de 260.401 (duzentos e sessenta mil quatrocentos e um) casos de fraude em telecomunicações. Estes registos abrangem diversas tipologias, cuja caracterização detalhada será apresentada nas secções subsequentes.

Para o efeito, o INCM procede à recolha sistemática de dados de tráfego e, recorrendo a ferramentas avançadas de análise de dados, realiza a verificação de comportamentos anómalos que consubstanciam fraudes ou tentativas de fraude nas redes dos operadores.

Esta operação permite assegurar uma fiscalização efectiva da actuação dos operadores, especialmente na implementação de mecanismos para detecção e bloqueio de tráfego fraudulento, contribuindo para a mitigação do impacto das práticas ilícitas e para a protecção da integridade das redes de comunicações electrónicas.

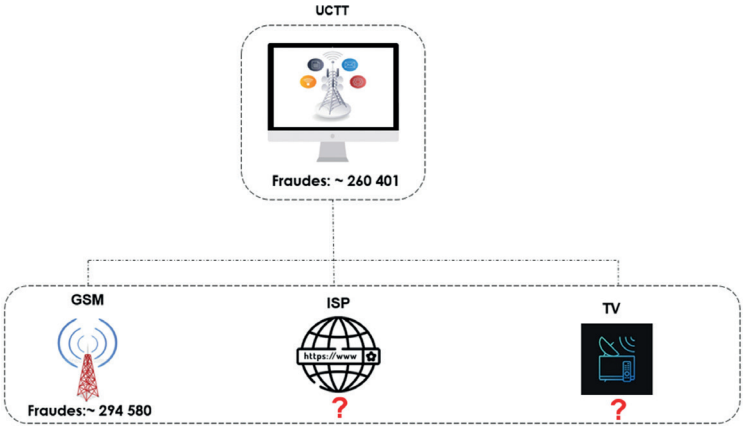


Figura 7 - Plataforma de Controlo de Tráfego de Telecomunicações

4.1.2. Operadores de Telecomunicações

Nos termos do Regulamento de Controlo de Tráfego de Telecomunicações e do Regulamento de Segurança de Redes de Telecomunicações, os operadores de telecomunicações em Moçambique estão legalmente obrigados a adoptar e implementar mecanismos destinados à prevenção e ao combate de fraudes nas suas redes. Adicionalmente, devem submeter, de forma regular e em formato definido pela Autoridade Reguladora, relatórios detalhados sobre as situações de fraude detectadas ou bloqueadas.

Durante o ano de 2024, os operadores de telefonia móvel reportaram um total de 294.580 (duzentos e noventa e quatro mil quinhentos e oitenta) casos de fraude em telecomunicações. Estas ocorrências resultam da monitoria interna conduzida pelos operadores, através dos seus sistemas de detecção e prevenção de fraudes, bem como das denúncias apresentadas pelos subscritores, que permitem identificar, em tempo útil, práticas fraudulentas que comprometem a segurança e a fiabilidade dos serviços prestados.

A análise detalhada dos tipos de fraude reportados pelos operadores será apresentada nas secções seguintes, com o objectivo de caracterizar os principais padrões e tendências observados ao longo do período em análise.

4.1.3. Plataforma de Denúncias

A Plataforma de Denúncia de Fraudes com Recurso a Redes de Telecomunicações ou Meios de Pagamento Electrónico é uma iniciativa conjunta da Autoridade Reguladora das Comunicações de Moçambique (INCM), da Procuradoria-Geral da República (PGR), do Banco de Moçambique, do Serviço Nacional de Investigação Criminal (SERNIC), da Associação Moçambicana de Bancos (AMB), das operadoras de telefonia móvel, de associações de crédito e de sociedades financeiras. Lançada oficialmente em Fevereiro de 2022, esta plataforma tem como objectivo fortalecer os mecanismos de combate às fraudes nos sectores das telecomunicações e dos serviços financeiros electrónicos.

Desde o seu lançamento, a Plataforma de Denúncias registou um total de 4.208 (quatro mil duzentas e oito) denúncias de fraude no sector das telecomunicações, sendo as mais recorrentes do tipo SMS. No ano de 2024, foram reportadas 500 (quinhentas) ocorrências, submetidas por 430 (quatrocentos e trinta) denunciantes.

Relativamente aos canais utilizados para a prática de fraudes, as redes sociais destacam-se como o meio frequente, seguidas das mensagens SMS. Em termos de distribuição geográfica, a província de Maputo registou o maior número de denúncias, com um total de 170 (cento e setenta) casos, enquanto a província do Niassa apresentou o menor número, com apenas 13 (treze) ocorrências.

A plataforma tem-se revelado uma ferramenta crucial na luta contra as fraudes, complementando os mecanismos automatizados de detecção e permitindo que os consumidores dos serviços públicos de telecomunicações participem activamente na denúncia de ocorrências fraudulentas, reforçando a confiança e a segurança do ecossistema digital nacional.

Actualmente, o acesso à plataforma é feito via internet, através do endereço https://fraude-denuncias.pgr.gov.mz. Estão igualmente em curso processos de avaliação com vista a garantir maior abrangência, através da integração com os serviços de SMS, USSD e outras plataformas digitais relevantes.

A seguir, é apresentado o *dashboard* com os dados da plataforma relativos ao ano de 2024.

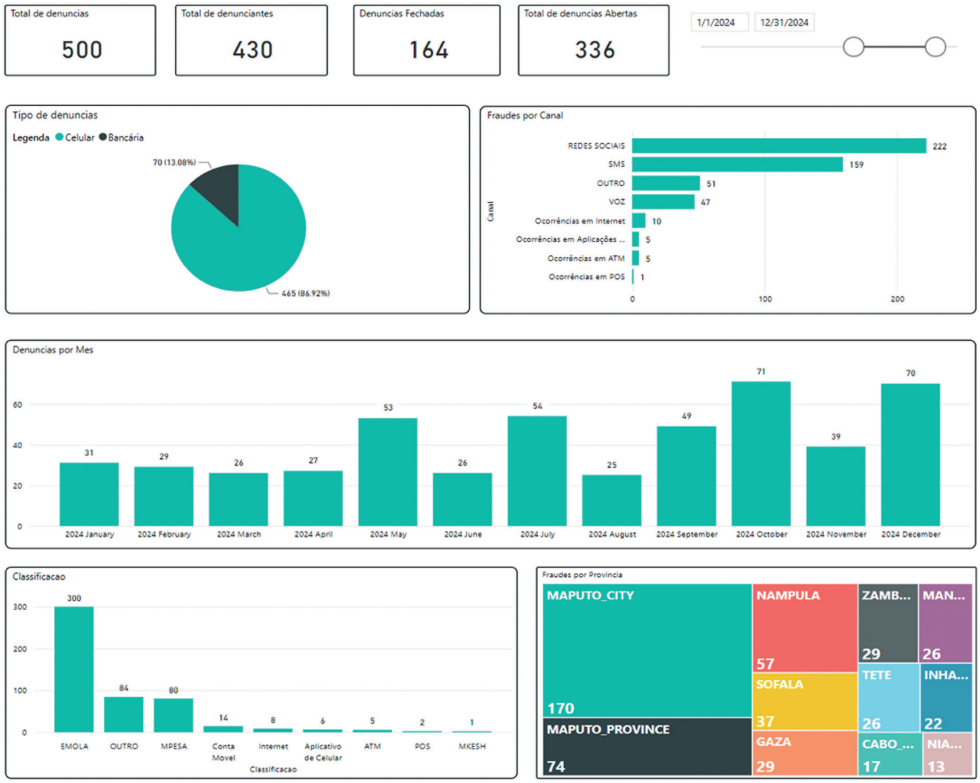


Figura 8 - Dashboard da Plataforma denúncias, data 10 de Janeiro de 2025

4.2. Distribuição de Fraudes – Fonte de dados

Durante o ano de 2024, foram registadas 555.481 (quinhentas e cinquenta e cinco mil quatrocentas e oitenta e uma) ocorrências de fraude no sector das telecomunicações, com origem em três principais fontes de reporte.

Os operadores de telefonia móvel reportaram 294.580 (duzentos e noventa e quatro mil quinhentos e oitenta) casos, correspondendo a 53,0% do total, identificados através dos seus sistemas internos de monitoria e prevenção de fraudes. A Autoridade Reguladora identificou 260.401 (duzentos e sessenta mil quatrocentos e uma) ocorrências, representando 46,9%, associadas sobretudo a fraudes técnicas e de larga escala, detectadas por meio da Plataforma de Controlo de Tráfego. Por fim, a Plataforma de Denúncias, alimentada por utilizadores finais, registou 500 (quinhentos) casos, o que corresponde a 0,1% do total.

A distribuição observada evidencia a complementaridade entre os mecanismos institucionais e os canais de participação pública, sublinhando a necessidade de reforçar a cooperação interinstitucional e a capacidade de resposta coordenada, com vista a combater, de forma eficaz, estas práticas ilícitas.

A seguir, apresenta-se o gráfico comparativo que ilustra a distribuição das ocorrências de fraude por fonte de reporte.

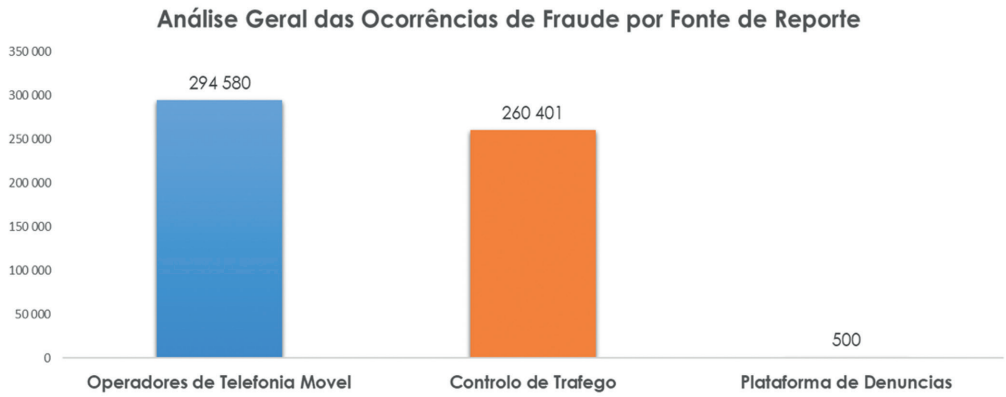


Figura 9 - Distribuição de Fraudes
Fonte INCM

4.3. Distribuição das Fraudes – Tipo de Fraudes e Fonte de Dados

A tabela seguinte apresenta os dados consolidados das ocorrências de fraude registadas no sector das telecomunicações durante o ano de 2024. Os dados reflectem, de forma desagregada, os diferentes tipos de fraudes identificados ao longo do período em análise, bem como as fontes responsáveis pelo respectivo reporte.

Este levantamento permite aferir não apenas a prevalência relativa de cada tipo de fraude, mas também o papel desempenhado por cada mecanismo de reporte na detecção e comunicação dos incidentes, contribuindo para uma avaliação mais precisa do panorama de ameaças que incidem sobre o ecossistema das comunicações electrónicas no país.

Importa destacar que a maior parte das ocorrências foi reportada pelos operadores de telefonia móvel e pela Autoridade Reguladora, evidenciando a sua relevância enquanto fontes primárias de detecção e resposta. Por outro lado, o número relativamente reduzido de casos registados através da Plataforma de Denúncias sublinha a necessidade de investir em acções de sensibilização e na promoção da confiança junto dos utilizadores finais, de modo a estimular a sua participação activa na identificação e denúncia de práticas fraudulentas.

Tipos de Fraudes	Operadores	Regulador	Plataforma Denúncia	Total
SIM-BOX	72 385	22 000	0	94 385
SIM-SWAP	529	1		530
SMS-Phishing	2466	235 000	250	237 716
VOICE-Phishing		1000	200	1 200
Registo	208 878	2400		211 278
WANGIRI IRSF	593			593
API Boundle	102			102
Mobile Money	108		50	158
Ataque Cibernetico	2			2
Engenharia Social	9501			9501
Internal Fraud	16			16
Total	294 580	260 401	500	555 481

Tabela 7 - Distribuição de Fraudes

4.4. Análise das Fraudes mais Comuns

A análise das ocorrências de fraude no sector das telecomunicações durante o ano de 2024 permitiu identificar os cinco tipos de fraude mais frequentes, que, em conjunto, totalizam 554.080 (quinhentas e cinquenta e quatro mil e oitenta) casos, representando 99,93% do total geral reportado.

A fraude por registo indevido de cartões SIM ocupa a primeira posição em termos de volume, com 211.278 (duzentos e onze mil duzentos e setenta e oito) ocorrências, correspondendo a 38,03% do total. No entanto, em termos de prevalência percentual, a fraude por SMS Phishing (Smishing) lidera, com 237.716 (duzentos e trinta e sete mil setecentos e dezasseis) casos, o equivalente a 42,79% das ocorrências.

A fraude por SIM-Box surge em terceiro lugar, com 94.385 (noventa e quatro mil trezentos e oitenta e cinco) ocorrências, representando 16,99%. Em seguida, destaca-se a engenharia social, com 9.501 casos (nove mil quinhentos e um), o que corresponde a 1,71%. Por fim, o Voice Phishing (Vishing), com 1.200 (mil e duzentas) ocorrências, equivalente a 0,22%.

Esta concentração demonstra que cinco tipologias de fraude dominam o panorama nacional, exigindo priorização de acções de prevenção, investigação e resposta específica, face à sua elevada incidência e ao impacto potencial nas redes de comunicações.

Estas fraudes reflectem as principais ameaças ao sector, com uma distribuição desigual das ocorrências, evidenciada de forma mais clara no gráfico seguinte, que facilita a análise e apoio à definição de estratégias de mitigação e prevenção.

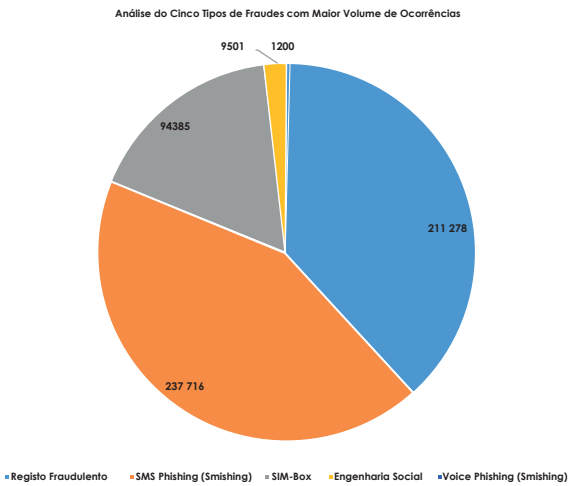


Figura 10 - Distribuição dos Principais Tipos de Fraudes, Fonte INCM

4.5. Volume e Frequência de Fraudes

Esta secção apresenta a análise do volume e da frequência dos incidentes de fraude registados em 2024, com base nos dados consolidados das três fontes de reporte.

4.5.1. Estimativa Por Período

Com o objectivo de proporcionar uma visão mais detalhada da distribuição temporal dos incidentes de fraude, procedeu-se à estimativa do volume médio de ocorrências por mês, por dia e por hora. Esta análise permite identificar padrões de frequência ao longo do tempo e apoiar a definição de estratégias de prevenção e resposta mais eficazes por parte das entidades competentes.

Os valores apresentados correspondem a médias estimadas, calculadas com base numa distribuição uniforme dos 555.481 (quinhentos e cinquenta e cinco mil, quatrocentos e oitenta e um) incidentes registados ao longo de 2024, considerando um total de 365 (trezentos e sessenta e cinco) dias. Segue-se, de seguida, a representação gráfica dos indicadores acima mencionados.

Figura 11 - Distribuição de Estimativa de Fraudes por Período
Fonte INCM

O gráfico apresentado acima ilustra a distribuição temporal dos incidentes de fraude ao longo de diferentes períodos. Os valores são organizados da seguinte forma:

- **Anual:** 555.481 (quinhentos e cinquenta e cinco mil, quatrocentos e oitenta e um) – representa o total de incidentes de fraude registados em 2024, englobando todas as tentativas e ocorrências identificadas durante o período de 12 (doze) meses.
- **Mensal:** 46.290 (quarenta e seis mil, duzentos e noventa) – corresponde à média mensal de fraudes registadas, calculada a partir do total anual, reflectindo o volume médio de incidentes de fraude por mês.
- **Diária:** 1.521 (mil, quinhentos e vinte e um) – indica a média de fraudes detectadas por dia, obtida pela divisão da média mensal de 46.290 ocorrências por 30 dias (valor médio de um mês).
- **Hora:** 63 (sessenta e três) – corresponde à média horária de fraudes, resultante da divisão da média diária de 1.521 ocorrências pelas 24 horas do dia.

4.5.2. Incidência de Fraudes por Consumidores

Com o intuito de avaliar o impacto das fraudes sobre os consumidores de serviços públicos de telecomunicações, foi calculada a incidência média de fraudes por consumidor. O cálculo teve por base o número total de incidentes de fraude reportados em 2024 e o número estimado de consumidores no país.

Dados Utilizados:

- Número total de incidentes de fraude em 2024; e
- Número total de subscritores de serviços públicos de telecomunicações.

Cálculo da Incidência

A incidência média de fraudes por consumidor foi calculada pela seguinte fórmula:

$$\textbf{Incidência por consumidor} = \frac{\text{Total de incidentes de fraude}}{\text{Número total de subscritores}}$$

Substituindo pelos valores:

$$\textbf{Incidência por consumidor} = \frac{555\ 481}{21.000.000}$$

Incidência por consumidor = 0,0264

Interpretação dos Resultados:

A incidência média de fraudes por consumidor foi de 0,0264 incidentes ao longo do ano. Este valor significa que, em média, ocorre um (1) incidente de fraude por cada 38 consumidores. Em termos relativos, representa aproximadamente 2,64% da população de consumidores afectados por fraudes em telecomunicações, anualmente.

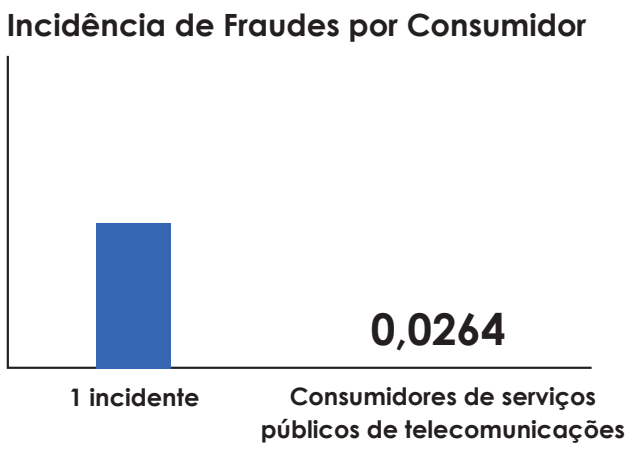


Figura 12 Gráfico de Incidência de Fraude por Consumidor de Serviços de Telecomunicações

4.5.3. Incidência Por Base Temporal

A tabela seguinte apresenta os valores médios estimados para cada intervalo temporal, calculados com base nas ocorrências reportadas ao longo do período em análise.

Base de Análise	Incidência Média por Consumidor
Anual	0,0264 fraudes por consumidor
Mensal	0,0022 fraudes por consumidor
Diária	0,000072 fraudes por consumidor

Tabela 8 Incidência de Fraude por Base Temporal

Interpretação:

- Estima-se que, anualmente, cada consumidor seja alvo de 0,026 incidentes ou tentativas de fraude, o que corresponde a um (1) incidente por cada 38 (trinta e oito) consumidores;
- Em termos mensais, este valor equivale a 1 incidente por cada 454 (quatrocentos e cinquenta e quatro) consumidores, aproximadamente;
- Diariamente, verifica-se cerca de 1 incidente por cada 13.800 (treze mil e oitocentos) consumidores.

4.6. Indicadores da Taxa de Sucesso de Fraudes

Em 2024, registaram-se 838.154 (oitocentos e trinta e oito mil, cento e cinquenta e quatro) tentativas de fraude, das quais 555.481 (quinhentas e cinquenta e cinco mil, quatrocentas e oitenta e uma) resultaram em fraudes bem-sucedidas, o que corresponde a uma taxa de sucesso de 66,3%.

A fórmula utilizada para o cálculo é a seguinte:

$$\textbf{Taxa de Sucesso (\%)} = \frac{\text{Fraudes bem-sucedidas}}{\text{Tentativa de Fraudes}} * 100$$

$$\textbf{Taxa de Sucesso (\%)} = \frac{555\ 48}{838\ 154} * 100$$

$$\textbf{Taxa de Sucesso (\%)} = 63\%$$

Este índice revela que, embora os mecanismos de prevenção estejam em funcionamento, uma parcela significativa das tentativas de fraude continua a resultar em sucesso. Tal evidência sublinha a necessidade de uma revisão aprofundada dos sistemas de detecção e resposta, com vista a reduzir ainda mais a taxa de sucesso das fraudes e a reforçar a segurança das infra-estruturas envolvidas.

4.7. Indicadores de Origem e Mecanismo

Esta secção visa apresentar uma análise detalhada da origem dos incidentes de fraude e dos mecanismos utilizados na sua execução. A identificação das fontes de origem e das me-

todologias aplicadas permite compreender as dinâmicas subjacentes às práticas fraudulentas no sector das telecomunicações, contribuindo para o desenho de respostas mais eficazes por parte das entidades reguladoras, operadores e utilizadores.

4.7.1. Distribuição Geográfica

A distribuição geográfica das fraudes por província revela que Nampula, Maputo-cidade e Maputo-província concentram 87% dos casos reportados a nível nacional.

A província de Nampula lidera com 249.764 (duzentos e quarenta e nove mil setecentas e sessenta e quatro) ocorrências, representando 45% do total, impulsionadas principalmente pela fraude de registo de cartões SIM, com 207.478 (duzentos e sete mil quatrocentos e setenta e oito) casos, e pela fraude por SIM-BOX, com 25.000 (vinte e cinco mil) ocorrências.

Maputo-cidade regista 165.806 (cento e sessenta e cinco mil, oitocentos e seis) casos, o equivalente a 30% do total, destacando-se pelo volume de *SMS-Phishing*, com 120.000 (cento e vinte mil) ocorrências, e de SIM-BOX, com 40.000 (quarenta mil) casos.

Já a província de Maputo apresentou 67.928 (sessenta e sete mil novecentos e vinte e oito) casos, correspondendo a 12% do total, com incidência elevada de *SMS-Phishing*, que totalizou 50.000 (cinquenta mil) ocorrências, e de SIM-BOX, com 15.000 (quinze mil) casos.

O volume significativo de fraudes nestas três províncias reforça a necessidade de medidas de segurança mais rigorosas, incluindo campanhas de sensibilização dirigidas e o aprimoramento dos mecanismos de detecção, monitoria e prevenção, com vista a proteger os utilizadores e salvaguardar a integridade das redes de comunicações nestas zonas de maior risco.

Província	SMS--Phishing	Registo	SIM-BOX	SIM--SWAP	Voice Phishing	WAN-GIRI	API Bundle	Mobile Money	Soc. Engi-neering	Internal Fraud	Cyber Attack	TOTAL
Nampula	15.000	207.478	25.000	150	300	200	0	50	1.500	0	0	249.764
Maputo Cidade	120.000	1.000	40.000	250	400	150	102	60	4.000	16	2	165.806
Maputo Província	50.000	500	15.000	80	200	100	0	30	2.000	0	0	67.928
Sofala	12.000	800	5.000	40	100	50	0	10	800	0	0	18.809
Gaza	10.000	700	3.000	30	80	40	0	5	700	0	0	14.561
Zambézia	8.000	400	2.000	15	50	30	0	2	400	0	0	10.900
Tete	6.000	200	1.500	10	40	15	0	1	300	0	0	9.067
Manica	5.000	100	1000	5	20	5	0	0	200	0	0	6.331
Inhambane	5.000	50	800	0	10	3	0	0	200	0	0	6.063
Cabo Delgado	6.716	50	1.085	0	0	0	0	0	200	0	0	8.051
TOTAL	237.716	211.278	94.385	580	1.200	593	102	158	9.501	16	2	555.481

Tabela 9 - Distribuição de Fraudes por Província, Fonte INCM

4.7.2. Técnicas e Canais de Fraude

A análise das fraudes reportadas no sector das telecomunicações em 2024 revela que as técnicas mais utilizadas pelos atacantes incluem a engenharia social e a fraude técnica, designadamente o *spoofing* (falsificação de identidade digital).

Os canais preferenciais para a execução destas fraudes continuam a ser as redes móveis,

com destaque para a utilização de mensagens SMS e chamadas telefónicas, que possibilitam o aliciamento e manipulação directa dos utilizadores.

As fraudes mais comuns, como o *SMS-Phishing*, o registo fraudulento de cartões SIM e a fraude por *SIM-Box*, caracterizam-se por uma elevada incidência, reflectindo o foco dos atacantes na exploração de vulnerabilidades estruturais das redes móveis e na manipulação da identidade dos utilizadores.

A tabela seguinte resume as principais técnicas de fraude identificadas e os canais preferenciais utilizados pelos atacantes para a sua execução.

Tipo de Fraude	Ocorrências Totais	Técnica Principal	Canal Preferencial
SMS-Phishing (Smishing)	237.716	Engenharia Social	SMS
Registo Fraudulento (SIM)	211.278	Fraude de Identidade	Rede Móvel
SIM-Box	94.385	Fraude Técnica (Spoofing)	Rede Móvel
Engenharia Social	9.501	Manipulação Psicológica	Redes Móveis, SMS
Voice-Phishing (Vishing)	1.200	Engenharia Social	Chamadas Telefónicas

Tabela 10 - Técnica e Canais Utilizados para Fraudes

4.8. Proliferação de Equipamentos Terminais não Homologados

EEsta secção analisa os principais desafios enfrentados pelo sector das telecomunicações, em virtude da utilização de equipamentos terminais não homologados, os quais, directa ou indirectamente, favorecem a ocorrência de actividades fraudulentas.

Durante o período em análise, não foram identificados casos de pirataria de equipamentos terminais em Moçambique, ou seja, não se registaram ocorrências formais e sistematizadas relativas à contrafacção de dispositivos móveis. Contudo, persistem práticas ilícitas associadas a estes dispositivos, destacando-se a alteração de códigos IMEI e a comercialização de equipamentos não homologados.

De acordo com os dados disponíveis, estima-se que circulam no mercado cerca de 10.200.000 (dez milhões e duzentos mil) equipamentos não homologados ou com IMEI adulterados. Este número corresponde a aproximadamente 30% do total de terminais em circulação, configurando uma parte significativa do mercado de dispositivos móveis. Esses aparelhos têm sido amplamente utilizados na prática de diversas actividades fraudulentas no sector das telecomunicações.

É importante destacar que, até o momento, os operadores de telecomunicações ainda não implementaram medidas eficazes para bloquear dispositivos que não cumpram os padrões estabelecidos pelo INCM. Esta lacuna pode contribuir directamente para a continuidade de práticas fraudulentas e constitui um risco à integridade do ecossistema das telecomunicações no país.

4.9. Alguns Exemplos de Casos de Fraudes Detectadas e Reportadas

Esta secção apresenta alguns casos de fraudes identificados no sector das telecomunicações ao longo de 2024. Entre os incidentes mais recorrentes e impactantes destacam-se os

registos indevidos de cartões SIM, a utilização de equipamentos *SIM-Box* e ataques de *SMS Phishing*. A seguir, descrevem-se os principais tipos de fraude registados:

4.9.1. Registo Fraudulento de cartão SIM

Em Maio de 2015, foi desmantelado, no bairro de Namicopo, na cidade de Nampula, um esquema de registo indevido de cartões SIM, conforme ilustrado nas imagens abaixo:

Figura 13 - Documentos Falsos Usados para Registo Fraudulento em Nampula

Figura 14 - Terminais Usados para Validação de Cartões SIM

Figura 15 - Bancadas do Escritório Clandestino
Fonte: https://www.youtube.com/watch?v=-ULM0O_k1fE

4.9.2. SMS Phishing

Os defraudadores, recorrendo a técnicas de engenharia social, têm explorado diversas iniciativas para cometer fraudes no sector das telecomunicações. Entre as abordagens mais comuns destacam-se: ofertas falsas de emprego, anúncios de prémios de concursos inexistentes, promoções fraudulentas de pacotes de dados a preços bonificados, sorteios simulados e outras estratégias enganosas.

Estas mensagens têm como objectivo induzir os utilizadores a fornecer dados pessoais ou a aceder a *links* maliciosos, como ilustrado nas imagens abaixo.

Figura 16 - Burlas de Sorteio de Prémios

5

IMPACTO DAS FRAUDES, SITUAÇÃO SOCIAL E MUDANÇAS CLIMÁTICAS SOBRE A SEGURANÇA, RESILIÊNCIA E DISPONIBILIDADE DAS COMUNICAÇÕES

5. Impacto das Fraudes, Situação Social e Mudanças Climáticas Sobre a Segurança, Resiliência e Disponibilidade das Comunicações

5.1. Impacto das fraudes

A presente secção apresenta a análise do impacto das fraudes, distribuídas por diversas modalidades e reportadas pelos operadores, pela Plataforma de Controlo de Tráfego e pelos canais formais de denúncia. Estas fraudes evidenciam diferentes níveis de complexidade, variando quanto à sua natureza, grau de sofisticação técnica e impacto económico, social e operacional.

5.1.1. Impacto económico

A estimativa do impacto económico foi apurada com base nos dados reportados pelos operadores de telecomunicações e demais entidades envolvidas, tendo em conta as características específicas de cada modalidade de fraude, os volumes afectados e as tarifas em vigor no mercado nacional.

Nos casos em que não foram submetidos dados completos à Autoridade Reguladora, não foi possível proceder à quantificação do impacto económico correspondente, limitando-se a análise às modalidades de fraude para as quais informação disponível permitiu uma estimativa fiável e tecnicamente fundamentada.

O impacto financeiro global estimado, resultante das ocorrências registadas ao longo do ano de 2024 e abrangendo os prejuízos suportados pelos operadores, pela Autoridade Reguladora e pelos consumidores, situa-se na ordem de 63.332.090,00 MZN (sessenta e três milhões trezentos e trinta e dois mil e noventa Meticais), o que corresponde a cerca de 1.000.000,00 USD (um milhão de dólares americanos).

A seguir apresenta-se a tabela com os procedimentos e critérios utilizados no cálculo dos valores associados a cada modalidade de fraude.

Tipo de Fraude	Informação Relacionada
Fraude por SIM-BOX	Foram registados 94.385 incidentes. Considerando um tempo médio de 20 minutos por chamada, estima-se que o volume total de tráfego fraudulento tenha sido de 1.887.700 minutos. Com uma tarifa de 7,50 Meticais por minuto, a perda financeira estimada é de 14.157.750,00 Meticais, representando receitas que deixaram de ser cobradas pelas operadoras.
Fraude por SIM-SWAP	Foram reportados 530 casos. Com base nas investigações e denúncias, estima-se um impacto financeiro total de 950.000,00 Meticais.
Fraude por Exploração Indevida de Pacotes API (API Bundle)	Foram identificados 102 casos, correspondendo a perdas financeiras estimadas em 42.000.000,00 Meticais, devido à exploração abusiva de pacotes tarifários associados a interfaces de programação (API).
Fraude no Registo de Cartões SIM	Verificaram-se 207.478 ocorrências de registo fraudulento de cartões SIM. Em cada activação ilícita, os agentes recebiam um incentivo de 30 Meticais, resultando numa perda financeira estimada de 6.224.340,00 Meticais.

Tabela 11 - Relação do Impacto económico

5.1.2. Impacto Social

As fraudes registadas no sector das telecomunicações em Moçambique, para além do impacto económico, apresentam implicações significativas a nível social e da segurança do Estado, nomeadamente:

- **Comprometimento da segurança do Estado**, dificultando a rastreabilidade de comunicações associadas a actividades ilícitas, o que enfraquece os mecanismos de investigação criminal e de prevenção de ameaças à ordem pública.
- **Violação da privacidade e dos direitos dos consumidores**, através da utilização indevida de dados pessoais em práticas como o *SIM-SWAP* e o registo indevido de cartões SIM.
- **Redução da confiança dos utilizadores nos serviços de telecomunicações** e nas instituições do sector, o que pode desencorajar a adesão a procedimentos formais de registo e autenticação digital.
- **Agravamento da exclusão digital**, sobretudo entre as populações mais vulneráveis, em virtude do receio de exposição a fraudes ou da apropriação indevida de identidades.
- **Comprometimento da qualidade dos serviços**, resultante do uso indevido das redes por meio de esquemas como o *SIM-BOX*, afectando negativamente a experiência dos utilizadores legítimos.
- **Desestruturação das cadeias de distribuição informal**, através da instrumentalização de agentes e revendedores por redes fraudulentas, prejudicando o desenvolvimento de iniciativas de micro-empreendedorismo no sector.

5.1.3. Impacto Operacional

As fraudes no sector das telecomunicações exercem um impacto significativo nas operações dos operadores, com repercussões que afectam a eficiência das redes, a qualidade do serviço e os custos operacionais. Entre os principais efeitos operacionais, destacam-se:

- **Sobrecarga das infra-estruturas de rede**, resultante do uso indevido de recursos, como no caso das fraudes *SIM-BOX*, comprometendo a capacidade de atender os utilizadores legítimos e reduzindo a eficiência da rede em períodos de maior procura.
- **Aumento dos custos operacionais**, decorrente da necessidade de implementar medidas adicionais de monitorização, segurança e prevenção para combater as fraudes.
- **Degradação da qualidade do serviço**, uma vez que a sobrecarga de tráfego fraudulento afecta a velocidade e a estabilidade das conexões, prejudicando a experiência dos clientes e aumentando a taxa de insatisfação e de reclamações.
- **Distorção dos dados e relatórios operacionais**, dado que as fraudes podem manipular o volume de tráfego reportado e dificultar a correcta análise de desempenho das redes e dos serviços prestados.
- **Comprometimento das operações de manutenção e gestão da rede**, uma vez que a detecção e resolução de fraudes exigem tempo e atenção, desviando recursos que poderiam ser alocados a melhorias ou actualizações da infra-estrutura.

5.2. Riscos Ambientais

Em 2024, o país foi atingido por três ciclones tropicais (Chido, Dikeledi e Jude) que afectaram gravemente a infra-estrutura de telecomunicações nas províncias de Cabo Delgado, Nampula e Niassa. Paralelamente, a ocorrência de manifestações violentas dificultou as operações de recuperação e de restabelecimento dos serviços em alguns distritos, agravando os danos causados pelas intempéries e comprometendo a continuidade dos serviços de comunicações.

5.2.1. Ciclone Chido

O Ciclone Chido causou danos significativos nas redes de telecomunicações, afectando múltiplos distritos nas províncias de Cabo Delgado, Nampula e Niassa. A tabela seguinte resume os principais impactos e os custos estimados de reposição associados.

Parâmetro	Descrição / Valores
Data do Evento	15 de Dezembro de 2024
Nome do Ciclone	Chido
Categoria Estimada	Categoria 4 (estimativa com base na velocidade dos ventos)
Velocidade Máxima dos Ventos	Até 215 km/h
Províncias Afectadas	Cabo Delgado, Nampula, Niassa
Distritos Mais Atingidos	Pemba, Nacala, Montepuez, Chiúre, Mueda, Macomia, Lichinga, Cuamba, entre outros
Sites de Telecomunicações Afectados	Cabo Delgado: 148
	Nampula: 56
	Niassa: 30
	Total: 234
	3 localidades afectadas com destruição total de torres
Torres Destruídas	Cortes de fibra óptica
Danos Identificados	Falhas nos rádios de microondas
	Interrupções extensas nas redes móveis e fixas
	Queda de postes de transmissão
	Falhas severas de energia eléctrica
Duração da Interrupção dos Serviços	Entre 24 e 96 horas nas áreas críticas
Impacto nos Serviços Críticos	Hospitais, centros de comando distritais, unidades de socorro e estações de rádio comunitárias
Medidas de Resposta Imediata	Activação de equipas de manutenção de emergência e unidades móveis de conectividade
Custos Estimados de Reposição (Total)	678.067.135,14 MZN
	10.479.499,97 USD
Fonte dos Dados	Relatórios submetidos pelas operadoras e inspecções técnicas coordenadas pelo regulador nacional

Tabela 12 - Impacto do Ciclone Chido

Figura 17 - Estação de Rádio-Base da Tmcel sem referência

5.2.2. Ciclone Dikeledi

O ciclone Dikeledi, ocorrido a 14 de Janeiro de 2025, afectou a província de Nampula, provocando interrupções nos serviços devido a cortes de energia e danos em sistemas de alimentação solar. Foram também reportados 150 km de fibra óptica danificados. A tabela seguinte apresenta um resumo dos principais impactos identificados e dos custos estimados reportados por uma das operadoras.

Parâmetro	Descrição / Valores
Data do Evento	14 de Janeiro de 2025
Nome do Ciclone	Dikeledi
Província Afectada	Nampula
Distritos Mais Atingidos	Angoche, Mossuril, Nacala e Ilha de Moçambique
Sites Afetados por Falta de Energia	109 sites afectados
Danos Identificados	Danos em sistemas de alimentação solar
	150 km de fibra óptica danificados pela queda de postes
Interferências Externas	Dificuldades logísticas causadas por barricadas em consequência das manifestações violentas
Infraestruturas Físicas Danificadas	Não foram reportados danos directos às infraestruturas das operadoras, com excepção da fibra óptica
Custos Estimados de Reposição	85.650,00 USD (valor estimado por uma única operadora)
Fonte dos Dados	Informação submetida por uma operadora e verificação parcial de campo pelo regulador nacional

Tabela 13 - Impacto do Ciclone Dikeledi

Figura 18 - Posto Administrativo de Murrebué: Site da Vodacom

5.2.3. Ciclone Jude

Em Março de 2025, o ciclone Jude voltou a afectar a província de Nampula, provocando a inoperacionalidade de mais de 500 *sites*, cortes extensos de fibra óptica e falhas generalizadas nos *links* de microondas. O acesso limitado, a falta de energia eléctrica e a escassez de combustível agravaram ainda mais a situação. A tabela seguinte resume os principais danos reportados e os custos de reposição estimados.

Parâmetro	Descrição / Valores
Data do Evento	Março de 2025
Nome do Ciclone	Jude
Província Afectada	Nampula
Sites Fora de Serviço	526 sites inoperacionais reportados por uma das operadoras
Danos Identificados	Corte de fibra óptica (142 km)
	Falhas generalizadas nos links de microondas
Condições que Agravaram a Situação	Falta de acesso às zonas afectadas
	Interrupções no fornecimento de energia eléctrica
	Escassez de combustível
Infraestruturas Físicas Danificadas	Fibra óptica e sistemas de conectividade remota via microondas
Custos Estimados de Reposição	146.323,63 USD (valor estimado por uma única operadora)
Fonte dos Dados	Relatório submetido por uma operadora e verificação preliminar conduzida pelo regulador

Tabela 14 - Impacto do Ciclone Jude

Figura 19 Estação de Rádio-Base da Movitel

5.2.4. Custos dos Ciclones nas Telecomunicações

Os ciclones Chido, Dikeledi e Jude provocaram prejuízos significativos às infra-estruturas de telecomunicações, com destaque para danos em *sites* técnicos, cortes de fibra óptica, falhas no fornecimento de energia e interrupções generalizadas de serviço. A tabela 15 apresenta uma consolidação parcial dos custos de reposição reportados pelas operadoras, totalizando aproximadamente 10.711.473,60 USD (dez milhões setecentos e onze mil quatrocentos e setenta e três dólares americanos e sessenta cêntimos).

Ciclone	Valor (MZN)	Valor (USD)
Chido	678.067.135,14	10.479.499,97
Dikeledi	Não disponível	85.650,00
Jude	Não disponível	146.323,63
Total	Parcial	10.711.473,60

Tabela 15 - Custo total do impacto dos ciclones

6 ACÇÕES E MEDIDAS DE MITIGAÇÃO

6. Acções e Medidas de Mitigação

6.1. Acções Implementadas

Em resposta à crescente incidência de fraudes no sector das telecomunicações, foram implementadas diversas acções destinadas a mitigar os impactos económicos, sociais e operacionais, reforçar a segurança e resiliência das redes, e restaurar a confiança dos consumidores. As medidas adoptadas incidiram, principalmente, sobre a prevenção, detecção e penalização das práticas fraudulentas, bem como no incentivo da colaboração entre os diversos actores do sector. As principais acções concretizadas incluem:

- **Bloqueio de Números Fraudulentos**

Os operadores procederam ao bloqueio de 208.878 (duzentos e oito mil, oitocentos e setenta e oito) cartões SIM, identificados como estando envolvidos em actividades fraudulentas, com o intuito de interromper as operações ilegais e proteger a integridade das redes de telecomunicações.

- **Processos Disciplinares**

Foram instaurados processos disciplinares a seis (6) colaboradores dos operadores, cujo envolvimento em actividades fraudulentas foi confirmado. Estas medidas visaram responsabilizar os indivíduos envolvidos e garantir a conformidade com as normas do sector.

- **Processo Judicial**

Foram instaurados processos judiciais a mais de 27 (vinte e sete) indivíduos, envolvidos no registo fraudulento de cartões SIM nas províncias de Nampula e outras regiões do país.

- **Reuniões de Colaboração entre o Regulador e Operadores**

O regulador tem mantido reuniões regulares com os operadores de telecomunicações, com o objectivo de elaborar modelos de mecanismos de partilha de informações e promover a colaboração entre as partes. Essas reuniões têm sido cruciais para melhorar a troca de dados e facilitar uma resposta mais eficaz às fraudes.

- **Inquérito sobre a Maturidade dos Operadores**

O Regulador realizou um inquérito para avaliar o nível de maturidade dos operadores de telecomunicações no que respeita à segurança e prevenção de fraudes, com o objectivo de identificar áreas de melhoria e reforçar as capacidades do sector para enfrentar as ameaças existentes.

• Seminário sobre Segurança e Resiliência nas Comunicações

Em coordenação com a Procuradoria-Geral da República (PGR), o Regulador organizou um seminário sobre segurança e resiliência nas comunicações. O evento teve como objectivo sensibilizar os operadores e a sociedade civil sobre a importância de reforçar a segurança e a resiliência nas infra-estruturas de telecomunicações.

• Encerramento de Rádios Comunitárias

O INCM procedeu à notificação formal de três estações de rádio e estabeleceu mecanismos de colaboração para a resolução do problema técnico identificado.

6.2. Medidas de Mitigação

Tendo em conta a natureza recorrente e em constante evolução das fraudes no sector das telecomunicações, encontra-se em curso a implementação de diversas medidas de mitigação com o objectivo de reduzir a exposição das redes e dos consumidores a práticas ilícitas, reforçar os mecanismos de controlo e promover uma resposta proactiva às ameaças identificadas. Estas acções, desenvolvidas em estreita coordenação entre o Regulador e os operadores, incluem:

a) Estabelecimento de uma Equipa de Resposta a Incidentes no Sector das Telecomunicações (ERIST)

Foram realizadas reuniões técnicas com todos os operadores de serviços públicos de telecomunicações para discussão da norma que orienta a criação da ERIST. O documento foi consensualmente aprovado pelos sectores envolvidos e encontra-se, neste momento, em fase de apreciação pelo Conselho de Administração, com vista à sua posterior publicação.

b) Implementação do Decreto n.º 23/2023, relativo ao Registo de Subscritores

Encontra-se em curso a implementação do regulamento aprovado pelo Decreto n.º 23/2023, que introduz medidas rigorosas para o registo de subscritores de serviços públicos de telecomunicações, incluindo a componente de registo biométrico. Esta iniciativa tem como objectivo assegurar a associação inequívoca do cartão SIM ao respectivo titular, facilitando a responsabilização individual em casos de envolvimento em práticas ilícitas.

As principais acções actualmente em implementação no âmbito deste decreto incluem:

- **Limitação do Número de Cartões SIM por Titular:** O Decreto estabelece um limite para o número de cartões SIM que podem ser registados com base no mesmo documento de identificação, contribuindo para a redução do uso abusivo de múltiplos números em actividades criminosas;
- **Obrigatoriedade de Prova de Vida para Subscritores:** Passa a ser exigida, de forma pe-

riódica, a realização de prova de vida por parte dos consumidores de serviços públicos de telecomunicações, como mecanismo de controlo para prevenir registos fraudulentos em nome de terceiros.

c) Expansão da Plataforma de Denúncias:

Encontra-se em curso a avaliação de propostas técnicas para a expansão da plataforma de denúncias, actualmente disponível apenas via internet. Pretende-se alargar o acesso através de serviços USSD e SMS, tornando a plataforma acessível a todos os consumidores, independentemente da sua conectividade à internet.

d) Quadro Legal:

O INCM tem intensificado os esforços para combater as actividades ilícitas relacionadas com a emissão de sinais de rádio não autorizados, visando garantir a qualidade e a segurança dos serviços de telecomunicações no país.

7 CONCLUSÕES

7. Conclusões

O ano de 2024 revelou-se particularmente desafiante para o sector das telecomunicações em Moçambique, no domínio da segurança e prevenção de fraudes. Os dados apurados evidenciam uma elevada incidência de práticas ilícitas, com destaque para fraudes baseadas em engenharia social e na exploração técnica de vulnerabilidades estruturais.

Foram reportadas 555.481 (quinhentas e cinquenta e cinco mil, quatrocentas e oitenta e uma) ocorrências, que representam não apenas um risco significativo para os consumidores, operadores e para o Estado, mas também sublinham a necessidade urgente de reforço das capacidades institucionais e tecnológicas.

As principais tipologias de fraude observadas foram o *SMS-Phishing*, o registo fraudulento de cartões SIM e o desvio de tráfego por *SIM-BOX*, que, em conjunto, representaram mais de 97% do total de incidentes registados. A elevada taxa de sucesso das fraudes (66,3%) reflecte tanto a sofisticação dos métodos utilizados como as fragilidades persistentes nos sistemas de autenticação, monitoria e controlo das redes.

O impacto económico estimado, superior a 63.000.000,00 MZN (sessenta e três milhões de meticais), constitui um indicador da magnitude das perdas sofridas, agravadas pelos efeitos sociais e operacionais, que comprometem a confiança nas comunicações, a qualidade dos serviços prestados e a eficácia dos mecanismos de responsabilização institucional e empresarial.

Apesar dos esforços encetados, como o bloqueio de cartões SIM, o início da implementação do registo biométrico e a criação da Equipa de Resposta a Incidentes de Segurança no sector das Telecomunicações (ERIST) — os resultados obtidos permanecem aquém das necessidades reais de um sector cada vez mais digital e exposto a riscos complexos e multidimensionais.

A análise evidencia a necessidade de investimentos contínuos, de maior cooperação entre entidades públicas e privadas e da adopção de uma abordagem estratégica multissectorial para garantir a resiliência e segurança das infra-estruturas de telecomunicações em Moçambique.

Em termos temporais, os incidentes podem ser analisados sob diferentes escalas. Foram registados, ao longo do ano, 555.481 (quinhentos e cinquenta e cinco mil quatrocentos e oitenta e um) incidentes, o que corresponde a:

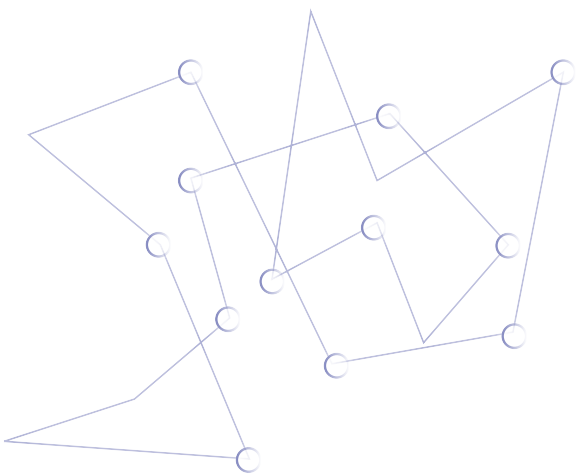
- 46.290 (quarenta e seis mil, duzentos e noventa) incidentes por mês;
- 1.521 (mil quinhentos e vinte e um) incidentes por dia; e
- Uma média de 63 (sessenta e três) incidentes por hora.

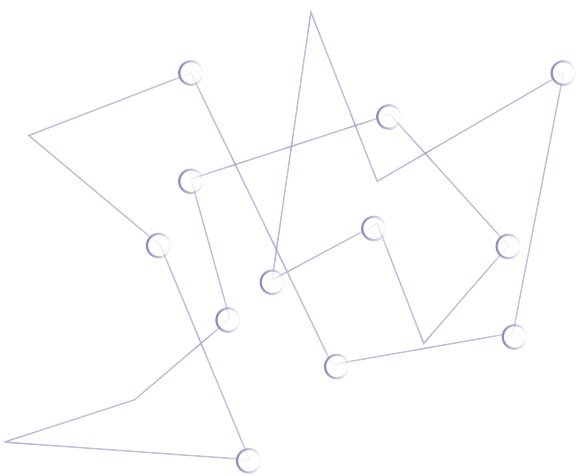
Este padrão de incidência evidencia a frequência alarmante de ocorrências de fraudes no sector, com destaque para a fraude por *SIM-BOX*, a mais recorrente, seguida das ocorrências de *SIM-SWAP*, exploração indevida de pacotes API e registo fraudulento de cartões SIM.

Adicionalmente, a existência de milhões de equipamentos não homologados em circulação demonstra a necessidade de reforçar os mecanismos de fiscalização e promover campanhas de sensibilização sobre os riscos associados a dispositivos não certificados.

Quanto à resiliência das infra-estruturas, especialmente no que respeita a fenómenos climáticos extremos, como os ciclones, esta revelou-se igualmente uma preocupação central. As condições adversas impactaram negativamente a disponibilidade dos serviços, provocando danos consideráveis nas redes de telecomunicações, sobretudo nas zonas mais vulneráveis do país. O valor global estimado para a reposição dos danos nas infra-estruturas afectadas, que

ascendeu a cerca de 10,7 milhões de dólares, evidencia a necessidade de reforçar a resiliência dos equipamentos e das redes para garantir a continuidade dos serviços essenciais, mesmo perante eventos climáticos extremos.





8. Recomendações

Com base na análise técnica, estatística e legal do presente relatório, são formuladas as seguintes recomendações estratégicas, com vista ao reforço da segurança nas comunicações electrónicas, mitigação de fraudes e protecção dos consumidores:

- **Reforço da capacidade técnica e institucional dos operadores:** os operadores devem investir em tecnologias avançadas, como inteligência artificial e big data, para detecção, monitoria e resposta a fraudes, bem como estabelecer centros de vigilância em tempo real que assegurem reacções céleres a incidentes e ameaças.
- **Aceleração da implementação do Decreto n.º 23/2023, sobre o Registo de Subscritores:** cumprir rigorosamente a limitação de cartões SIM por titular e assegurar a realização periódica da prova de vida para prevenir fraudes no registo.
- **Fortalecimento da colaboração interinstitucional e partilha de informações:** formalizar protocolos de cooperação entre o Regulador, o SERNIC, a Procuradoria-Geral da República e instituições do sector financeiro, promovendo a criação de uma base nacional integrada de incidentes de fraude, com acesso reservado às entidades competentes, para partilha segura de dados e inteligência, nos termos do artigo 6 do Regulamento de Segurança de Rede de Telecomunicações.
- **Expansão e Integração da Plataforma Nacional de Denúncias:** colaborar tecnicamente com o Regulador na expansão da plataforma, incorporando canais de acesso alternativos (USSD e SMS) e assegurando a sua universalização. Adicionalmente, promover campanhas de sensibilização junto dos consumidores, reforçando a confiança nos mecanismos de denúncia.
- **Promoção da literacia digital e sensibilização pública:** o Regulador deve promover programas regulares de educação digital, com foco na prevenção de fraudes, segurança de dados pessoais e boas práticas no uso de tecnologias móveis.
- **Revisão e conformidade com o quadro legal e regulamentar:** os operadores devem manter-se actualizados e em conformidade com as normas e regulamentos vigentes, promovendo a sua integração nos procedimentos operacionais. Devem, ainda, apoiar iniciativas de revisão legislativa que visem o agravamento das penalizações e a celeridade dos processos judiciais relativos a crimes cibernéticos e fraudes nas comunicações.
- **Combate ao uso de terminais não homologados:** os operadores devem adoptar mecanismos eficazes de controlo, bloqueio e dissuasão do uso de dispositivos não homologados nas suas redes. É igualmente recomendada a colaboração activa com as autoridades alfandegárias e policiais, visando a mitigação da entrada e comercialização destes equipamentos no mercado nacional.

Glossário

Fraudes em Telecomunicações (ITU/UIT): actividades ilícitas que exploram vulnerabilidades em redes e serviços de telecomunicações para obter ganhos financeiros, causar prejuízos aos operadores, consumidores ou Estados, ou burlar sistemas de segurança.

Fraudes em Telecomunicações (GSMA): exploração intencional de vulnerabilidades em redes móveis para obter benefícios financeiros, causar perdas aos operadores, clientes ou interromper serviços legítimos.

Tráfego Fraudulento (Decreto 38/2023) Regulamento de Controlo de Tráfego de Telecomunicações: todo o tráfego gerado, terminado, guardado ou em trânsito, não identificado, que tenha sido modificado ou indesejado, contribuindo para a defraudação dos interesses do Estado, operadores, subscritores ou sociedade em geral.

Defraudador: é o indivíduo que, de forma deliberada e fraudulenta, pratica actos com o objectivo de enganar, prejudicar ou obter vantagens ilícitas à custa de outrem, violando normas legais ou contratuais.

Operadores/Operadoras: de acordo com o Regulamento de Controlo de Tráfego de Telecomunicações, aprovado pelo Decreto n.º 38/2023, um operador de telecomunicações é qualquer sociedade comercial, licenciada pela Autoridade Reguladora das Comunicações em Moçambique, que se dedique à prestação de serviços de telecomunicações.

Registo Fraudulento de Cartão SIM: é o acto doloso que consiste na activação ou registo de um cartão de identificação de assinante (SIM) mediante a utilização de dados pessoais falsos, forjados, pertencentes a terceiros sem o seu consentimento, ou obtidos por meios ilícitos, com o propósito de ocultar a identidade real do utilizador, iludir os mecanismos legais de controlo e identificação, ou facilitar a prática de infracções, nomeadamente burla, extorsão, usurpação de identidade ou outras actividades de natureza fraudulenta.

Fraude por *phishing* via SMS/Chamadas: é uma prática ilícita que consiste na utilização de mensagens escritas (SMS) ou chamadas telefónicas com o objectivo de induzir os destinatários, por meio de engano ou manipulação, a facultarem voluntariamente informações confidenciais, como credenciais de acesso, dados bancários, palavras-passe ou códigos de segurança.

Fraude por desvio de tráfego (*SIMBOX*): é uma prática ilegal que consiste na terminação de chamadas internacionais como se fossem chamadas locais, mediante a utilização de dispositivos denominados SIMBOX (caixas de cartões SIM), os quais contém múltiplos cartões de operadoras nacionais.

Fraude por exploração de vulnerabilidades (*API Bundle*): refere-se à utilização de falhas de segurança em interfaces de programação de aplicações (API) com o intuito de aceder, manipular ou interceptar dados de sistemas ou redes de telecomunicações de forma não autorizada.

Fraude por clonagem de cartões SIM (SIM Swap Fraud): é um tipo de fraude que envolve a manipulação ilícita do processo de troca de um cartão SIM, com o intuito de obter controlo sobre o número de telefone de uma vítima.

Fraude por chamadas internacionais Premium Rate (*IRS Fraud*): é uma prática fraudulenta que envolve a criação e promoção de números de telefone com tarifação premium, normalmente utilizados para serviços internacionais, com o objectivo de gerar receitas ilícitas.

Fraude Por Moeda Electrónica (*Mobile Money*): refere-se a práticas fraudulentas que ocorrem no contexto de sistemas de pagamento digital móveis, conhecidos como mobile money, que permitem a transferência e o armazenamento de valores monetários através de dispositivos móveis.

Fraudes Internas (Internal Fraud): referem-se a actividades fraudulentas realizadas por indivíduos dentro de uma organização, como funcionários, colaboradores ou prestadores de serviços, com o intuito de beneficiar pessoalmente à custa da empresa ou da organização.

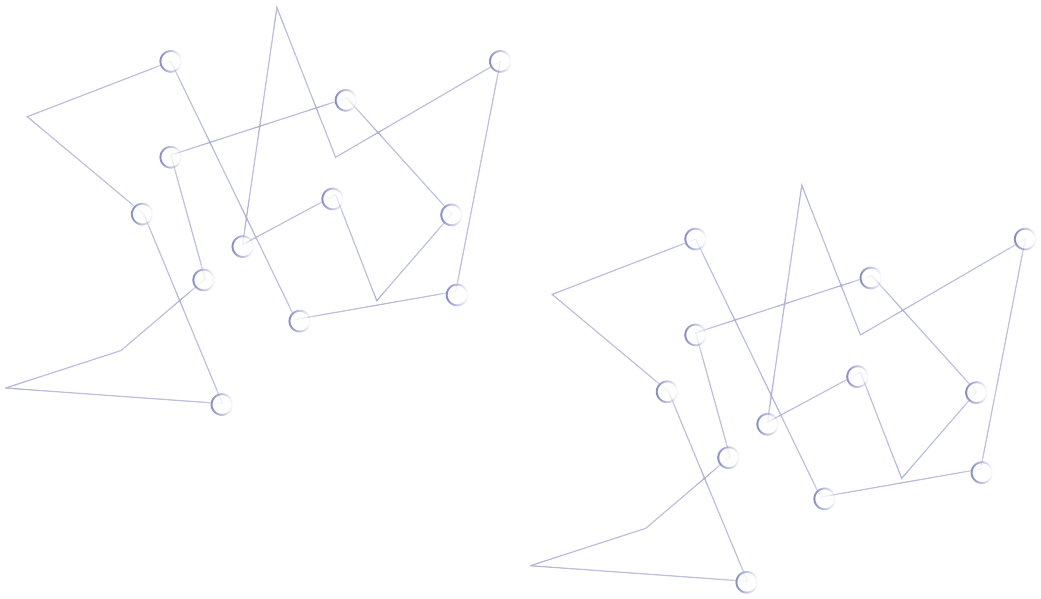
Engenharia Social: é um conjunto de técnicas fraudulentas que exploram o comportamento humano e a confiança das vítimas para obter informações sensíveis ou aceder a sistemas protegidos, sem recorrer a métodos técnicos de invasão.

Ataques Cibernéticos: referem-se a tentativas maliciosas de comprometer, danificar, ou interromper sistemas informáticos, redes de computadores ou infraestruturas digitais, através do uso de técnicas ou ferramentas informáticas. Estes ataques podem ser realizados por indivíduos, grupos ou entidades com intenções fraudulentas, incluindo o roubo de dados, sabotagem de sistemas, ou a disseminação de vírus e malware.

Terminais Homologado: dispositivos certificados pela Autoridade Reguladora para operar em redes nacionais.

Siglas

ITU/UIT - *International Telecommunication Union* (União Internacional de Telecomunicações).
ENISA - (Agência Europeia para a Segurança das Redes e da Informação)
GSMA - *Global System for Mobile Communications Association*
PGR - Procuradoria-Geral da República (Moçambique)
INCM - Instituto Nacional das Comunicações de Moçambique
SERNIC - Serviço Nacional de Investigação Criminal (Moçambique)
AMB - Associação Moçambicana de Bancos (parceira da Plataforma de Denúncias)
5G - Quinta geração de redes móveis (tecnologia de telecomunicações)
API - *Application Programming Interface* (Interface de Programação de Aplicações)
AIT - *Artificial Inflation of Traffic* (Inflação Artificial de Tráfego)
DCL - *Dynamic Code Loading* (Carregamento Dinâmico de Código)
GCI - *Global Cybersecurity Index* (Índice Global de Cibersegurança)
DDoS - *Distributed Denial of Service* (Ataque de Negação de Serviço Distribuído)
M-Pesa - Serviço de pagamento móvel (moeda electrónica)
MKesh - Serviço de pagamento móvel (moeda electrónica)
eMola - Serviço de pagamento móvel (moeda electrónica)
OTP - *One-Time Password* (Senha de Uso Único)
SIM - *Subscriber Identity Module* (Cartão de identificação do assinante)
SIMBOX - Dispositivo ilegal com múltiplos cartões SIM para desvio de tráfego
SMS - *Short Message Service* (Serviço de Mensagens Curtas)
SS7 - Protocolo de sinalização de redes móveis (alvo de ataques)
USSD - *Unstructured Supplementary Service Data* (Serviço de menus interactivos)
IMEI - *(International Mobile Equipment Identity)* Número único que identifica um dispositivo móvel na rede. É usado para reconhecer o equipamento, bloquear aparelhos roubados ou perdidos e apoiar o controlo pelas operadoras e autoridades.



INCM

Autoridade Reguladora das Comunicações