INCM
Autoridade Reguladora das Comunicações

RELATÓRIO SOBRE O NÍVEL DE MATURIDADE DA SEGURANÇA E RESILIÊNCIA DAS TELECOMUNICAÇÕES REFERENTE AO ANO DE 2024

Ficha Técnica:

Título: Relatório Sobre o Nível de Maturidade da Segurança e Resiliência das Telecomunicações Referente ao Ano de 2024
Autor: Instituto Nacional das Comunicações de Moçambique – INCM
Ano de Publicação: 2025
Revisão: Ídolo El
Layout e Paginação: Ídolo El
Tradução: Ídolo El

INCM
Autoridade Reguladora das Comunicações

RELATÓRIO SOBRE O NÍVEL DE MATURIDADE DA SEGURANÇA E RESILIÊNCIA DAS TELECOMUNICAÇÕES REFERENTE AO ANO DE 2024

Índice

Sumário Executivo....9
1. Introdução....12
1.1. Contextualização....12
1.2. Objectivos....12
1.3. Dimensões e Resultados Esperados....12
1.4. Referências e Enquadramento Normativo....13
1.5. Caracterização da Amostra....14
1.6. Métricas de Avaliação....15
2. Apreciação Geral do Nível de Maturidade por Subsector....17
2.1. Telefonia Móvel (MNO)....19
2.2. Provedores de Serviços de Internet (ISP)....20
2.3. Operadores de Serviços de Televisão (TV)....20
2.4. Implicações Estratégicas e Regulatórias....20
3. Apreciação Específica do Nível de Maturidade por Dimensão....22
3.1. Cooperação e Partilha de Informação....24
3.1.1. Apreciação Geral....24
3.1.2. Apreciação Detalhada por Subsector....25
3.1.3. Conclusão....26
3.1.4. Recomendações....27
3.2. Gestão de Fraudes....27
3.2.1. Apreciação Geral....28
3.2.2. Apreciação Detalhada por Subsector....29
3.2.3. Conclusão....31
3.2.4. Recomendações da Secção....31
3.3. Protecção de Dados e Privacidade....32
3.3.1. Apreciação Geral....33
3.3.2. Apreciação Detalhada por Subsector....34
3.3.3. Conclusão....35
3.3.4. Recomendações....36
3.4. Resiliência da Rede de Telecomunicações....37
3.4.1. Apreciação Geral....37
3.4.2. Apreciação Detalhada por Subsector....38
3.4.3. Conclusão....41
3.4.4. Recomendações....41
3.5. Controlos e Medidas de Segurança....42
3.5.1. Apreciação Geral....43
3.5.2. Apreciação Detalhada por Subsector....44
3.5.3. Conclusão....46
3.5.4. Recomendações....47
3.6. Preparação e Resposta a Incidentes....48
3.6.1. Apreciação Geral....48
3.6.2. Apreciação Detalhada por Subsector....49
3.6.3. Conclusão....51
3.6.4. Recomendações....52
3.7. Políticas, Processos e Procedimentos....53
3.7.1. Apreciação Geral....53

3.7.2. Apreciação Detalhada por Subsector....54
3.7.3. Conclusões....56
3.7.4. Recomendações....57
3.8. Consciencialização e Formação....58
3.8.1. Apreciação Geral....58
3.8.2. Apreciação Detalhada por Subsector....59
3.8.3. Conclusão....62
3.8.4. Recomendações....62
3.9. Melhoria Contínua....63
3.9.1. Apreciação Geral....63
3.9.2. Apreciação Detalhada por Subsector....65
3.9.3. Conclusão....67
3.9.4. Recomendações....67
4. Considerações Finais....69
4.1. Principais Constatações....70
4.2. Oportunidades de Melhoria....71
4.3. Recomendações Estratégicas....71
4.4. Conclusão....73

Lista de Gráficos

Gráfico 1: Comparação do Nível de Maturidade por Dimensão e Subsector....19
Gráfico 2: Nível de Maturidade Sectorial na Cooperação e Partilha de Informação....24
Gráfico 3: Nível de Maturidade Sectorial nas Fraudes....28
Gráfico 4: Nível de Maturidade Sectorial na Protecção de dados....33
Gráfico 5: Nível de Maturidade Sectorial na Resiliência....38
Gráfico 6: Nível de Maturidade Sectorial dos Controlos e Medidas de Segurança....43
Gráfico 7: Nível de Maturidade de Preparação e Resposta a Incidentes....49
Gráfico 8: Nível de Maturidade Sectorial das Políticas e Procedimentos....54
Gráfico 9: Nível de Maturidade Sectorial da Consciencialização....59
Gráfico 10: Nível de Maturidade Sectorial da Melhoria Contínua....64

Lista de Tabelas

Tabela 1: Dimensões Avaliadas e Resultados Esperados....9
Tabela 2: Resumo dos Resultados Gerais por Subsector....10
Tabela 3: Dimensões Avaliadas e Resultados Esperados....13
Tabela 4: Critério para Métricas de Avaliação....16
Tabela 5: Resumo dos Resultados Gerais por Subsector....18
Tabela 6: Indicadores de Cooperação....25
Tabela 7: Indicadores de Fraude....29
Tabela 8: Indicadores de Protecção de Dados....34
Tabela 9: Indicadores de Resiliência....39
Tabela 10: Indicadores de Controlos e Medidas de Segurança....44
Tabela 11:Indicadores de Preparação e Resposta a Incidentes....50
Tabela 12: Indicadores de Políticas, Processos e Procedimentos....55
Tabela 13: Indicador de Consciencialização e Formação....60
Tabela 14: Indicadores de Melhoria Contínua....65

Lista de Acrónimos e Siglas

CIS	*Center for Internet Security* (Centro para a Segurança da Internet)
COBIT	*Control Objectives for Information and Related Technologies*
Cloud	Computação em Nuvem
ENISA	*European Union Agency for Cybersecurity*
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusões)
IPS	*Intrusion Prevention System* (Sistema de Prevenção de Intrusões)
ISP	*IInternet Service Provider* (Provedor de Serviços de Internet)
ISO/IEC 27001	Norma Internacional para Sistemas de Gestão de Segurança da Informação
ISO/IEC 27002	Código de Boas Práticas para Controlos de Segurança da Informação
KPI	*Key Performance Indicator* (Indicador-Chave de Desempenho)
MNO	*Mobile Network Operator* (Operadora de Rede Móvel/Telefonia Móvel)
NIST CSF	*National Institute of Standards and Technology Cybersecurity Framework*
SIEM Security	*Informationand Event Management*
SIM Swap	Técnica Fraudulenta de Troca de Cartão SIM
TV	Operadores de Televisão

Sumário Executivo

O presente relatório apresenta resultados da avaliação da Segurança e Resiliência no sector das telecomunicações, conduzida com base num inquérito dirigido a 22 (vinte e dois) operadores, subdivididos em três (3) segmentos/subsectores, três (3) operadores de telefonia móvel (MNO), quatro (4) operadores do serviço de televisão (TV) e 15 (quinze) provedores de serviços de Internet (ISP), constituindo uma amostra representativa do sector das telecomunicações.

A avaliação incidiu sobre nove (9) dimensões, as quais serviram de referência para determinar o nível de maturidade cibernética e operacional dos operadores, conforme ilustrado na tabela seguinte:

Dimensão	Resultados Esperados
Cooperação e Partilha de Informação	Identificar o grau de colaboração entre os operadores e o regulador, avaliar a existência de canais formais de comunicação e partilha de alertas, e promover uma cultura de confiança mútua no sector.
Gestão de Fraudes	Verificar a existência de mecanismos internos de prevenção, detecção e resposta a fraudes, com vista à mitigação de riscos financeiros, reputacionais e operacionais.
Protecção de Dados e Privacidade	Avaliar se os operadores garantem a confidencialidade, integridade e legalidade no tratamento de dados pessoais dos utilizadores, em conformidade com a legislação vigente.
Resiliência das Redes de Telecomunicações	Determinar a capacidade das infraestruturas de telecomunicações para manterem os serviços activos durante falhas ou crises, incluindo estratégias de redundância, recuperação e continuidade operacional.
Controlos e Medidas de Segurança	Confirmar a implementação de medidas técnicas e organizacionais robustas de segurança, alinhadas com boas práticas internacionais, para protecção dos sistemas e dados sensíveis.
Preparação e Resposta a Incidentes	Avaliar a existência de planos de contingência, equipas de resposta a incidentes e exercícios de simulação, que assegurem reacções eficazes e coordenadas em caso de incidentes de segurança.
Políticas, Processos e Procedimentos	Verificar a existência de políticas formais e processos padronizados que regulem a gestão de riscos e a segurança da informação, bem como a sua efectiva aplicação no quotidiano organizacional.
Consciencialização e Formação	Medir o nível de sensibilização dos colaboradores face às ameaças cibernéticas, bem como a frequência e abrangência dos programas de formação contínua em segurança.
Melhoria Contínua	Identificar se as entidades possuem mecanismos de monitoria, auditoria e aperfeiçoamento sistemático das suas práticas de segurança, com base em indicadores e lições aprendidas.

Tabela 1: Dimensões Avaliadas e Resultados Esperados

A avaliação revelou tratar-se de um sector ainda em fase de transição, caracterizado por níveis de maturidade bastante heterogéneos entre os operadores, destacando-se as MNO pela excelência das suas práticas e pelo nível de maturidade superiores em relação aos demais segmentos do mercado de telecomunicações.

A tabela seguinte apresenta o resumo da avaliação efectuada, distribuída por dimensão e por segmentos dos operadores.

Dimensão	MNO	ISP	TV
Cooperação e Partilha de Informação	71%	21%	11%
Gestão de Fraudes	73%	20%	25%
Protecção de Dados e Privacidade	82%	53%	47%
Resiliência das Redes de Telecomunicações	75%	53%	62%
Controlos e Medidas de Segurança	98%	75%	90%
Preparação e Resposta a Incidentes	85%	55%	44%
Políticas, Processos e Procedimentos	81%	55%	44%
Consciencialização e Formação	74%	47%	34%
Melhoria Contínua	81%	53%	23%
Média	80%	48%	43%

Tabela 2: Resumo dos Resultados Gerais por Subsector

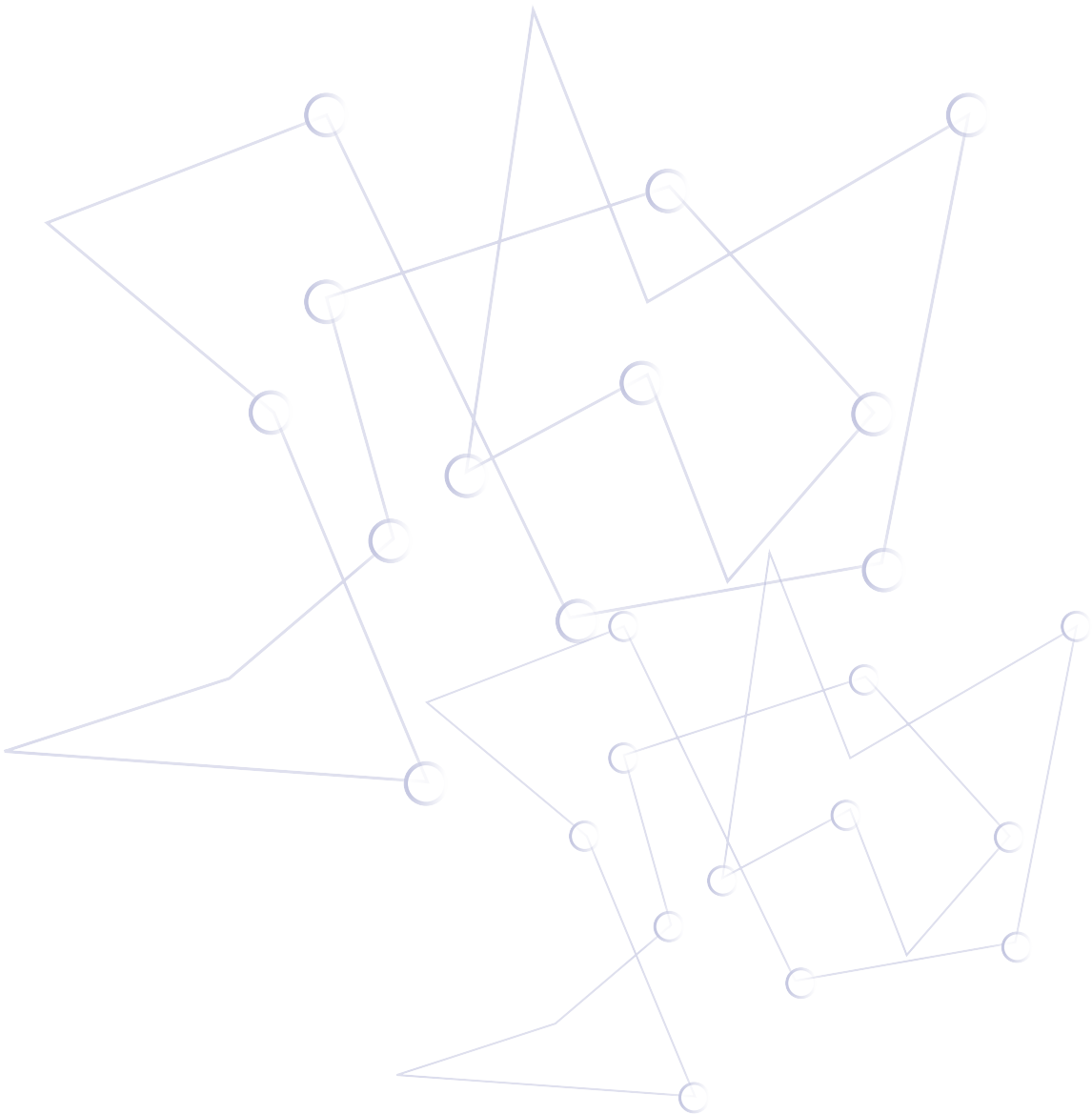
Os resultados evidenciam disparidades significativas nos níveis de maturidade entre os operadores dos diferentes subsectores. As MNO destacam-se com um desempenho global robusto (80%), liderando todas as dimensões avaliadas, em particular o Controlo e Medidas de Segurança (98%) e Protecção de Dados e Privacidade (82%). Em contraste, os ISP e os operadores de TV apresentam níveis de maturidade baixos, com médias de 48% e 43%, respectivamente. As fragilidades mais críticas concentram-se na Cooperação e Partilha de Informação (21% e 11%) e na Melhoria Contínua (53% e 23%). A média global do sector das telecomunicações, situada em 57%, revela a urgência de intervenções estruturadas que promovam o alinhamento normativo, operacional e tecnológico entre todos os subsectores.

Face a este cenário, recomenda-se uma actuação estratégica centrada na padronização de boas práticas, com destaque para a criação de protocolos técnicos obrigatórios e iniciativas permanentes de articulação com a Autoridade Reguladora, especialmente nos segmentos com menor nível de maturidade. A implementação de programas de capacitação contínua, ajustados às fragilidades identificadas, deve ser acompanhada por mecanismos de medição de impacto.

Reforça-se ainda a importância da adopção de tecnologias de monitoria contínua, bloqueios automatizados e inteligência artificial na gestão de fraudes e incidentes. A protecção de dados exige medidas transversais mais rigorosas, incluindo segurança em *cloud* e auditorias

regulares.

Por fim, propõe-se um acompanhamento regulatório activo, com avaliações sistemáticas e incentivos ao cumprimento das metas, de forma a promover a maturidade digital e garantir maior resiliência, confiança institucional e capacidade de resposta às ameaças emergentes no sector das telecomunicações.



1. INTRODUÇÃO

1.1. Contextualização

O sector das telecomunicações exerce um papel crucial na sociedade contemporânea, sendo vital para o desenvolvimento económico, a inclusão digital e a Segurança do Estado. À medida que a digitalização avança, intensificam-se igualmente os desafios associados à segurança cibernética, à protecção dos dados pessoais e à resiliência das infra-estruturas de telecomunicações.

A crescente complexidade e interdependência das infraestruturas de telecomunicações exigem um elevado grau de segurança e resiliência, de modo a garantir a continuidade dos serviços prestados à sociedade, num contexto global, marcado pelo acelerado avanço tecnológico e pelo aumento constante das ameaças cibernéticas, torna-se essencial que os operadores e prestadores de serviços de telecomunicações assegurem o pleno cumprimento das normas regulamentares vigentes e adoptem as melhores práticas internacionais.

1.2. Objectivos

O presente estudo tem como objectivo principal avaliar o nível de maturidade dos operadores e prestadores de serviços públicos de telecomunicações no cumprimento das normas regulamentares vigentes, com especial enfoque nos seguintes aspectos:

- **Disponibilidade**: Garantir que a rede esteja acessível aos consumidores, respeitando os níveis de serviço acordados;
- **Integridade**: Avaliar a protecção dos dados verificando se os mesmos são tratados salvaguardando medidas contra modificações não autorizadas;
- **Confidencialidade**: Avaliar a protecção dos dados verificando se os mesmos são tratados salvaguardando medidas contra acessos não autorizados;
- **Autenticidade**: Certificar que a origem dos dados transmitidos seja verificável;
- **Resiliência**: Avaliar a capacidade das redes em resistir a eventos adversos, adaptando-se e mantendo o seu funcionamento normal.

1.3. Dimensões e Resultados Esperados

A avaliação foi estruturada em nove (9) dimensões temáticas fundamentais, consideradas críticas, conforme apresentado na tabela seguinte:

Dimensão	Resultados Esperados
Cooperação e Partilha de Informação	Identificar o grau de colaboração entre os operadores e o regulador, avaliar a existência de canais formais de comunicação e partilha de alertas, e promover uma cultura de confiança mútua no sector.
Gestão de Fraudes	Verificar a existência de mecanismos internos de prevenção, detecção e resposta a fraudes, com vista à mitigação de riscos financeiros, reputacionais e operacionais.
Protecção de Dados e Privacidade	Avaliar se os operadores garantem a confidencialidade, integridade e legalidade no tratamento de dados pessoais dos utilizadores, em conformidade com a legislação vigente.
Resiliência das Redes de Telecomunicações	Determinar a capacidade das infraestruturas de telecomunicações para manterem os serviços activos durante falhas ou crises, incluindo estratégias de redundância, recuperação e continuidade operacional.
Controlos e Medidas de Segurança	Confirmar a implementação de medidas técnicas e organizacionais robustas de segurança, alinhadas com boas práticas internacionais, para protecção dos sistemas e dados sensíveis.
Preparação e Resposta a Incidentes	Avaliar a existência de planos de contingência, equipas de resposta a incidentes e exercícios de simulação, que assegurem reacções eficazes e coordenadas em caso de incidentes de segurança.
Políticas, Processos e Procedimentos	Verificar a existência de políticas formais e processos padronizados que regulem a gestão de riscos e a segurança da informação, bem como a sua efectiva aplicação no quotidiano organizacional.
Consciencialização e Formação	Medir o nível de sensibilização dos colaboradores face às ameaças cibernéticas, bem como a frequência e abrangência dos programas de formação contínua em segurança.
Melhoria Contínua	Identificar se as entidades possuem mecanismos de monitoria, auditoria e aperfeiçoamento sistemático das suas práticas de segurança, com base em indicadores e lições aprendidas.

Tabela 3: Dimensões avaliadas e resultados esperados

1.4. Referências e Enquadramento Normativo

A presente abordagem metodológica assenta num quadro normativo e regulamentar robusto, que reflecte o compromisso com elevados padrões de segurança e conformidade legal, tendo em consideração os instrumentos nacionais que estabelecem os princípios e obrigações fundamentais aplicáveis ao sector, com ênfase nos seguintes:

- Lei n.º 4/2016 (Lei das Telecomunicações);
- Decreto n.º 66/2019 (Regulamento de Segurança de Redes de Telecomunicações)
- Decreto n.º 38/2023 (Regulamento de Controlo de Tráfego

Este enquadramento foi, ainda, complementado por normas e boas práticas internacionalmente reconhecidas, com destaque para a ISO/IEC 27001 e a ISO/IEC 27002, as directrizes emi-

tidas pela ENISA (Agência da União Europeia para a Ciber segurança) e os controlos definidos pelo CIS (*Center for Internet Security*). A adopção articulada destes referenciais visa garantir a uniformidade e a fiabilidade dos procedimentos adoptados, assegurando simultaneamente a conformidade com os padrões internacionais em matéria de segurança da informação e protecção de dados.

1.5. Caracterização da Amostra

A presente avaliação contou com a participação de 22 (vinte e dois) operadores do sector das telecomunicações, abrangendo diferentes níveis de envolvimento no mercado. A amostra é composta pela seguinte distribuição:

- Três (3) Operadoras de Telefonia Móvel (MNO);
- Quinze (15) Provedores de Serviços de Internet (ISP);
- Quatro (4) Operadores de Serviços de Televisão (TV).

Para além da classificação por subsector, a caracterização da amostra incluiu variáveis estruturais e operacionais relevantes, as quais permitiram obter uma visão mais abrangente do perfil das entidades avaliadas. Abaixo detalham-se os principais aspectos considerados:

1. Número de Colaboradores

- A maioria dos operadores possui menos de 250 (duzentos e cinquenta) colaboradores;
- Um operador de telefonia móvel tem entre 501 (quinhentos e um) e 1.000 (mil) colaboradores;
- Alguns operadores dispõem de mais de 1.000 (mil) colaboradores.

2. Quantidade de Subscritores

- A maioria dos ISP e operadores de TV indicou possuir até 1.000 (mil) subscritores;
- Algumas entidades situam-se na faixa entre 1.001 (mil e um) e 50.000 (cinquenta mil) subscritores;
- Apenas as operadoras de telefonia móvel ultrapassam 500.001 (quinhentos mil e um) subscritores, o que confirma a sua posição hegemónica no mercado nacional.

3. Tecnologias de Armazenamento e Processamento de Dados

- O *data center* próprio é a tecnologia predominante, sendo utilizada por mais de metade das entidades inquiridas;
- As soluções como *disaster recovery* activo e serviços de *cloud* nacional apresentam também uma adopção significativa;
- As tecnologias alternativas, como *cloud internacional, data centers* partilhados e *disas-*

ter recovery passivo, registam uma utilização residual.

4. Localização Geográfica dos Centros de Operações

- A maioria das entidades declarou ter os seus centros de operações localizados na região Sul do país, com destaque para as cidades de Maputo, Xai-Xai e Vilankulo;
- Um número considerável de entidades indica igualmente presença nas regiões Centro e Norte, com incidência nas cidades da Beira, Nacala, Nampula e Tete.

5. Cobertura Territorial

- As operadoras móveis e alguns ISP reportaram dispor de cobertura nacional;
- A maioria dos ISP e operadores de televisão apresenta uma cobertura territorial limitada, operando sobretudo em centros urbanos ou em menos de cinco (5) cidades.

6. Estrutura da Direcção Máxima

- A estrutura mais comum é a Direcção-Geral, presente em mais de metade das entidades analisadas;
- O modelo de governação assente em Conselhos de Administração surge com maior frequência entre os MNO e as entidades de maior porte institucional.

Este enquadramento permite aferir, com rigor, o grau de representatividade da amostra, que, apesar de globalmente positivo, evidencia a necessidade de um maior comprometimento por parte do sector nas futuras avaliações. A consolidação da colaboração entre os operadores e a Autoridade Reguladora será determinante para garantir diagnósticos mais abrangentes, precisos e representativos do nível de maturidade em segurança e resiliência das telecomunicações no país.

1.6. Métricas de Avaliação

A avaliação baseou-se em escalas estruturadas, que permitiram medir, de forma objectiva, a percepção e o nível de implementação de práticas regulatórias pelos operadores do sector.

- **Percepção**: Utilizou-se uma escala de Likert (0 a 1), permitindo aferir o grau de concordância das entidades com afirmações sobre boas práticas.
- **Implementação**: Aplicou-se uma escala de 0, 0.5 ou 1, onde 0 representa o não cumprimento na totalidade, 0.5 cumprimento parcial e 1o cumprimento total, o que permitiu verificar a existência ou não de medidas concretas.

Respostas nulas ou não aplicáveis foram pontuadas com zero, assegurando a integridade dos resultados. Nas questões com múltiplas opções, a pontuação foi distribuída proporcionalmente com base no número de respostas seleccionadas. As pontuações foram depois classificadas segundo níveis de maturidade:

Nível de Maturidade	Pontos %)
Inicial	0–20
Básico	21–40
Intermédio	41–60
Avançado	61–80
Optimizado	81–100

Tabela 4: Critério para Métricas de Avaliação

Este modelo permitiu uma análise comparável e orientada para resultados, facilitando a identificação de boas práticas e de áreas com potencial de melhoria.

2

APRECIAÇÃO GERAL DO NÍVEL DE MATURIDADE POR SUBSECTOR

2. Apreciação Geral do Nível de Maturidade por Subsector

A avaliação do nível de maturidade em segurança e resiliência das telecomunicações em Moçambique revelou uma clara assimetria entre os subsectores que compõem o ecossistema nacional: MNO, ISP e TV. Esta disparidade reflecte diferentes estágios de conformidade, implementação de práticas de segurança e integração de mecanismos de resposta e prevenção, com impacto directo na robustez e resiliência global do sector.

Os resultados mostram um nível médio de maturidade de 57%, com variações significativas entre subsectores. As MNO apresentam maturidade elevada em quase todas as dimensões avaliadas, enquanto os ISP eoperadores de TV, revelam fragilidades que requerem medidas correctivas. A tabela seguinte resume os resultados médios por dimensão temática e subsector:

	MNO	ISP	TV
Cooperação e Partilha de Informação	71%	21%	11%
Gestão de Fraudes	73%	20%	25%
Protecção de Dados e Privacidade	82%	53%	47%
Resiliência das Redes de Telecomunicações	75%	53%	62%
Controlos e Medidas de Segurança	98%	75%	90%
Preparação e Resposta a Incidentes	85%	55%	44%
Políticas, Processos e Procedimentos	81%	55%	44%
Consciencialização e Formação	74%	47%	34%
Melhoria Contínua	81%	53%	23%
Média	80%	48%	43%

Tabela 5: Resumo dos Resultados Gerais por Subsector

O gráfico abaixo complementa essa análise, oferecendo uma leitura visual comparativa dos níveis de maturidade registados em cada uma das dimensões temáticas. Constata-se uma liderança clara das MNO, com percentagens superiores em todos os indicadores, contrastando com o desempenho substancialmente inferior dos ISP e, sobretudo, das TV. Esta diferenciação reforça a necessidade de uma abordagem regulatória diferenciada e estruturada, com vista à harmonização da maturidade cibernética entre todos os subsectores.

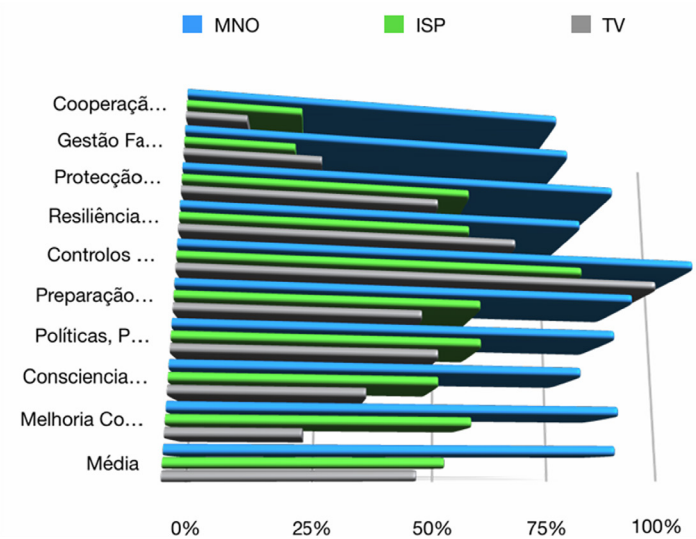


Gráfico 1: Comparação do Nível de Maturidade por Dimensão e Subsector

2.1. Telefonia Móvel (MNO)

As MNO apresentaram um desempenho substancialmente superior, com uma média global de 80%, evidenciando níveis avançados de conformidade e implementação em todas as dimensões avaliadas. Destacaram-se, em particular, nos domínios de Controlos de Segurança (98%), Protecção de Dados (82%) e Resposta a Incidentes (85%).

Este desempenho robusto assentou nos seguintes factores:

- Articulação eficaz com o regulador e existência de protocolos formais de cooperação em 100% dos casos;
- Implementação de sistemas automatizados de prevenção de fraudes, com bloqueios em tempo real, bases de dados de terminais suspeitos e equipas especializadas;
- Políticas consolidadas de protecção de dados, incluindo criptografia, auditorias regulares e controlos de acesso;
- Infraestruturas resilientes, com redundância plena e planos de continuidade operacionais;
- Equipas dedicadas à resposta a incidentes, com uso integral de soluções IDS/IPS;e
- Integração de processos de melhoria contínua, com auditorias, métricas de desempenho e envolvimento activo das partes interessadas.

As MNO revelaram uma clara internalização dos principais referenciais internacionais (ISO/IEC 27001, NIST CSF, CIS), assumindo-se como padrão de referência no contexto nacional.

2.2. Provedores de Serviços de Internet (ISP)

Com uma média global de 48%, os ISP posicionaram-se num nível intermédio de maturidade, caracterizado por esforços pontuais e iniciativas parcialmente estruturadas, mas com elevada heterogeneidade interna e ausência de práticas uniformizadas.

As principais debilidades incluem:

- Baixa formalização da cooperação institucional (30%) e articulação limitada com o regulador (25%);
- Ausência generalizada de mecanismos de bloqueio automático, bases de dados antifraude e acções coordenadas (20%);
- Políticas de protecção de dados com aplicação inconsistente e resposta débil a incidentes;
- Estratégias básicas de continuidade operacional, com falhas em redundância e partilha de informação;e
- Baixo investimento em formação, com acções esporádicas e cobertura limitada.

Estas vulnerabilidades expõem o segmento a riscos operacionais e de conformidade, exigindo uma intervenção regulatória orientada, padronização de processos e apoio técnico para a elevação da maturidade.

2.3. Operadores de Serviços de Televisão (TV)

O subsector de TV apresenta o nível mais baixo de maturidade, com média de 43%, resultado de fragilidades estruturais persistentes em todas as dimensões avaliadas. Entre os principais constrangimentos identificados destacam-se:

- Cooperação institucional quase inexistente (11%) e articulação mínima com o regulador;
- Ausência de sistemas antifraude estruturados e inexistência de responsáveis dedicados;
- Políticas formais de protecção de dados sem implementação prática verificável;
- Inexistência de planos formais de continuidade e resposta fragmentada a incidentes;
- Formação interna insuficiente, sem planos regulares nem mecanismos de avaliação; e
- Falta de processos de revisão, auditoria e integração de lições aprendidas.

A falta de recursos, capacitação e cultura organizacional voltada para a segurança e resiliência das redes de telecomunicações, coloca este subsector em situação de risco elevado, sendo prioritário o estabelecimento de requisitos mínimos obrigatórios, investimento técnico-financeiro e supervisão regulatória reforçada.

2.4. Implicações Estratégicas e Regulatórias

Com base nos resultados, recomendam-se as seguintes acções estratégicas para mitigar riscos, reduzir assimetrias e promover a resiliência das redes de telecomunicações:

- Definição de requisitos mínimos obrigatórios, adaptados à realidade operacional de

cada segmento;

- Criação de programas de certificação e capacitação específicos para os ISP e operadores de televisão;
- Reforço da fiscalização técnica e responsabilização institucional, com auditorias periódicas e relatórios públicos;
- Promoção da partilha intersectorial de boas práticas e tecnologias, com liderança do regulador; e
- Estímulo à cooperação multissectorial como mecanismo estruturante de confiança e resposta coordenada.

O fortalecimento da maturidade cibernética do sector constitui um imperativo para a segurança do Estado, a confiança dos utilizadores e a continuidade dos serviços essenciais no processo de digitalização de Moçambique.

3

APRECIAÇÃO ESPECÍFICA DO NÍVEL DE MATURIDADE POR DIMENSÃO

3. Apreciação específica do Nível de Maturidade por Dimensão

Este capítulo apresenta uma análise detalhada e específica sobre o nível de maturidade dos operadores do sector das telecomunicações em Moçambique, com base na informação recolhida junto dos diferentes subsectores.

Cada subcapítulo está estruturado em quatro componentes:

i. Avaliação geral do desempenho agregado dos subsectores analisados;
Nesta componente, apresenta-se uma visão global comparativa sobre o desempenho dos subsectores, identificando claramente quais apresentam um nível superior de maturidade operacional e aqueles com desempenho mais baixo, permitindo, assim, uma visão estratégica das áreas críticas que requerem atenção prioritária.

ii. Análise detalhada por indicador, permitindo identificar pontos fortes e fragilidades específicas;
Nesta análise são examinados, de forma minuciosa, cada um dos indicadores avaliados, destacando-se os aspectos em que cada subsector se distingue positivamente (pontos fortes), bem como as áreas onde se verificam lacunas e vulnerabilidades significativas (fragilidades específicas). Esta abordagem detalhada facilita uma compreensão aprofundada das práticas em vigor e das áreas prioritárias de intervenção.

iii. Conclusão da secção, que sintetiza os principais resultados e propõe linhas de orientação para o reforço da colaboração no sector;
A conclusão desta secção consiste num resumo estratégico dos principais achados, destacando as constatações mais relevantes e as lições aprendidas. Com base nestas conclusões, são definidas linhas de orientação específicas para promover e reforçar a colaboração e cooperação entre os diversos operadores e demais intervenientes, visando melhorar o desempenho geral do sector.

A apresentação de recomendações concretas orientadas para a melhoria dos mecanismos de cooperação e partilha de informação.

Finalmente, esta componente apresenta recomendações práticas, acionáveis e direccionadas especificamente para melhorar os mecanismos existentes de cooperação e partilha de informação entre os operadores, o regulador e outras entidades relevantes. Estas recomendações são elaboradas com base nas fragilidades identificadas, procurando fomentar um ambiente de maior confiança, transparência e eficiência no sector.

3.1. Cooperação e Partilha de Informação

Esta dimensão centra-se na análise do grau de colaboração entre operadores de telecomunicações e demais entidades relevantes, com base em seis (6) indicadores estratégicos. A avaliação procurou compreender em que medida existem mecanismos formais e eficazes de partilha de informação crítica, articulação com o regulador, gestão conjunta de incidentes e iniciativas de cooperação voltadas à mitigação de riscos e vulnerabilidades.

A análise também incluiu aspectos como a utilização de plataformas seguras para a troca de dados, as barreiras identificadas na comunicação interinstitucional, e a existência de práticas estruturadas de formação e sensibilização. Esta abordagem permitiu identificar os níveis de maturidade operacionais e o alinhamento dos operadores com os requisitos regulatórios, fornecendo subsídios concretos para o fortalecimento da confiança e da integração no ecossistema nacional de telecomunicações.

3.1.1. Apreciação Geral

O sector das telecomunicações, na dimensão cooperação e partilha de informação, revela, no seu conjunto, um nível de maturidade básico, com uma pontuação média global de 35%. Este resultado reflecte uma presença inicial de estruturas e processos relevantes, mas também grandes assimetrias entre os subsectores, sublinhando a necessidade de medidas estruturantes para promover a cooperação e a harmonização de práticas no sector.

O gráfico seguinte demonstra a distribuição do posicionamento dos subsectores quanto a esta dimensão.

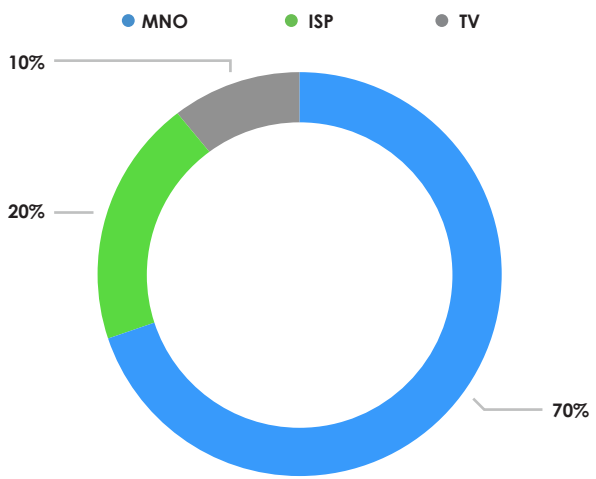


Gráfico 2: Nível de Maturidade Sectorial na Cooperação e Partilha de Informação

Dos 35% atribuídos a esta dimensão no cálculo do nível de maturidade geral, as operadoras de telefonia móvel (MNO) destacam-se como líderes, com 70% da contribuição, seguidas pelos provedores de serviços de Internet (ISP) com 20%, e pelos operadores de televisão (TV), com apenas 10%.

Este desempenho robusto das MNO evidencia a existência de processos consolidados, uma abordagem preventiva eficaz e uma postura activa de colaboração com o regulador e os demais actores do ecossistema.

No caso dos ISP, embora alguns revelem progressos pontuais, verifica-se uma grande assimetria entre as entidades, marcada por fragilidades estruturais e falta de uniformidade na adopção de boas práticas, especialmente em áreas como controlo de acessos, resposta a incidentes e articulação institucional.

Quanto ao segmento de televisão, a análise aponta para a ausência de políticas claras, escassa formalização de procedimentos e uma interacção limitada com o regulador, o que compromete significativamente a capacidade de resposta e a adaptação a riscos operacionais.

3.1.2. Apreciação detalhada por subsector

A presente secção apresenta uma visão comparativa e detalhada dos três subsectores analisados. Conforme demonstrado na tabela abaixo, são sintetizados os resultados por subsector, indicando a percentagem de operadores que adoptam práticas estruturadas nos domínios de cooperação institucional, relação com o regulador, partilha de infra-estruturas e segurança da informação.

Indicadores	ISP	TV	MNO
Mecanismos de Cooperação	30%	20%	100%
Colaboração com Regulador	25%	15%	73%
Partilha de Infraestruturas	15%	5%	100%
Partilha de Informação	15%	5%	53%
Medidas de Confidencialidade	20%	10%	67%
IGestão de Incidentes	20%	10%	53%
Média	21%	11%	74%

Tabela 6: Indicadores de Cooperação

De forma detalhada seguem as constatações conforme dados da tabela:

1. Mecanismos de Cooperação

As MNO apresentam 100% de adesão a protocolos formais de cooperação, enquanto que apenas 30% dos ISP e 20% das operadoras de televisão reportam estruturas similares, revelando

fragilidades significativas nos dois últimos subsectores.

2. Colaboração como Regulador

As MNO mantém uma relação próxima com o Regulador, com 73% a reportarem colaboração activa, enquanto os ISP e operadores de televisão revelam baixo envolvimento, com apenas 25% e 15% de participação, respectivamente, para além das obrigações formais.

3. Partilha de Infraestruturas

Na partilha de infraestruturas, as MNO atingem 100% de colaboração, enquanto os ISP e operadoras de TV registam níveis muito baixos, com 15% e 5% respectivamente, devido a conflitos comerciais e exclusividade de conteúdos.

4. Partilha de Informação

As MNO lideram na partilha de informação, com 53% a utilizarem sistemas estruturados. Os ISP operam com mecanismos básicos (15%) e as operadoras de TV mostram grande fragilidade, com apenas 5% a recorrerem a plataformas formais.

5. Medidas de Confidencialidade

Na protecção da informação, as MNO destacam-se com 67% a aplicarem criptografia avançada e auditorias regulares; O ISP ficam nos 20%, com medidas básicas, e as operadoras de TV mostram grandes lacunas, com apenas 10% a adoptarem políticas robustas.

6. Gestão de Incidentes

As MNO continuam a destacar-se, com 53% a utilizarem plataformas conjuntas para a gestão de incidentes entre operadores. Entre os ISP, 20% dispõem de planos básicos, e o segmento de TV evidencia respostas não estruturadas, com apenas 10% a actuar de forma planeada.

3.1.3. Conclusão

A análise da dimensão de Cooperação e Partilha de Informação evidenciou um sector ainda em fase inicial de maturidade, com destaque positivo para as MNO, que apresentam práticas bem estruturadas, elevada articulação com o regulador e mecanismos robustos de partilha e gestão de riscos. Em contrapartida, os ISP e, sobretudo, as TV enfrentam desafios relevantes como a ausência de protocolos formais, baixa participação institucional e fragilidades na protecção e transferência segura de dados sensíveis.

As disparidades observadas entre os subsectores revelaram a necessidade urgente de tra-

çar estratégias coordenadas que promovam a padronização de boas práticas, o reforço da confiança interinstitucional e a criação de plataformas conjuntas para resposta a incidentes e partilha de infra-estrutura. A harmonização destas práticas é fundamental para garantir a resiliência do ecossistema de telecomunicações e assegurar uma resposta sectorial mais integrada e eficaz perante ameaças cibernéticas e operacionais.

3.1.4. Recomendações

Com base nos resultados apurados, propõem-se as seguintes medidas prioritárias:

1. Reforçar os mecanismos formais de cooperação entre operadores, promovendo a assinatura de protocolos padronizados, especialmente nos subsectores menos integrados (ISP e TV);

2. Intensificar a articulação com o Regulador, através da promoção de fóruns sectoriais periódicos, submissão sistemática de dados e participação activa em iniciativas de capacitação e alinhamento estratégico;

3. Desenvolver linhas orientadoras específicas para a partilha de infraestrutura e conteúdos, clarificando regras e promovendo soluções colaborativas que mitiguem conflitos comerciais e preservem a concorrência;

4. Adoptar protocolos uniformes para a partilha segura de informação, incentivando a utilização de plataformas interoperáveis e a adopção de padrões mínimos obrigatórios nos subsectores mais atrasados;

5. Estabelecer requisitos mínimos de segurança da informação, com enfoque em medidas de confidencialidade, como criptografia, controlo de acessos e auditorias regulares, adaptadas à realidade de cada tipo de operador;

6. Institucionalizar mecanismos de gestão conjunta de incidentes, promovendo exercícios colaborativos, partilha de lições aprendidas e definição de planos sectoriais de resposta;

7. Desenvolver acções de sensibilização e capacitação técnica, com foco nos segmentos menos maduros, garantindo uma evolução gradual, mas sustentada da maturidade sectorial.

3.2. Gestão de Fraudes

A dimensão de Gestão de Fraudes avalia a capacidade dos operadores de telecomunicações para prevenir, detectar e responder a actividades fraudulentas que ameaçam a integridade dos serviços e a confiança dos utilizadores. Esta análise incide sobre oito indicadores-chave, cobrindo desde a existência de canais formais de denúncia e comunicação com o regulador, até à implementação de mecanismos técnicos como bloqueio de números, uso de bases de dados de terminais suspeitos e designação de equipas especializadas.

O objectivo central é aferir o grau de maturidade operacional dos diferentes subsectores — MNO, ISP e TV — e identificar as principais lacunas que limitam uma actuação eficaz e coor-

denada no combate às fraudes. A avaliação visa ainda fornecer subsídios para o reforço das capacidades internas dos operadores e para a adopção de estratégias de colaboração que permitam uma resposta integrada e sustentável a este tipo de ameaças.

3.2.1. Apreciação Geral

No âmbito da presente secção, o sector das telecomunicações obteve uma pontuação global de 39%, o que corresponde a um nível básico de maturidade no que respeita à prevenção, detecção e resposta a fraudes. Este resultado revela que, embora existam iniciativas relevantes em curso, o sector ainda enfrenta limitações estruturais e operacionais, especialmente nos segmentos com menor capacidade instalada.

O gráfico seguinte demonstra a distribuição do posicionamento dos subsectores quanto a esta dimensão.

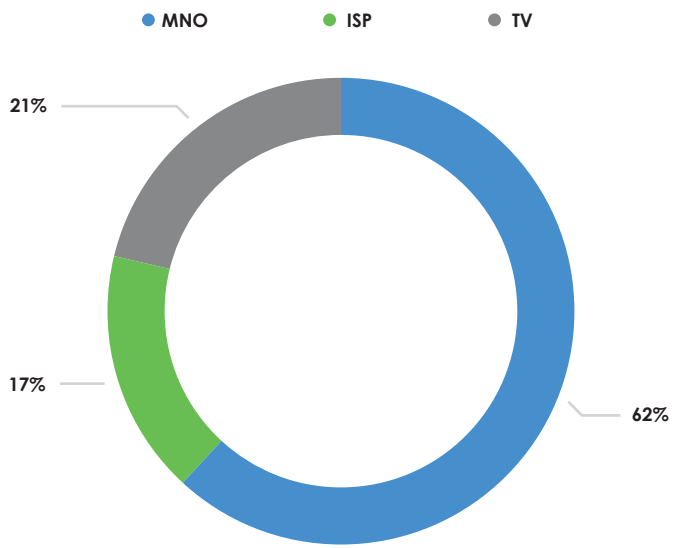


Gráfico 3: Nível de Maturidade Sectorial nas Fraudes

As MNO lideram o sector, com uma pontuação de 62% no nível de maturidade, seguidas pelas TV com 21%, ficando os ISP com a percentagem remanescente de 17%. O desempenho das MNO é sustentado pela adopção de sistemas automatizados de detecção, uma capacidade de resposta ágil e eficaz, bem como investimentos regulares em inovação tecnológica e segurança operacional.

Embora as TV apresentem menor exposição a riscos de fraude directa, os resultados revelam estruturas preventivas pouco desenvolvidas e no caso dos ISP, evidenciam disparidades significativas, sendo que a maioria dos operadores demonstram limitações na detecção, monitoria e tratamento eficaz de fraudes.

3.2.2. Apreciação Detalhada Por Subsector

Nesta subsecção são apresentados os indicadores relacionados com a gestão de fraudes nos três subsectores das telecomunicações, sendo que o objectivo é de proporcionar uma visão detalhada sobre os níveis de maturidade, práticas implementadas e áreas críticas que exigem reforço, conforme é apresentado na tabela abaixo.

	ISP	TV	MNO
Serviço de Denúncia	15%	25%	33%
Comunicação com o Regulador	8%	25%	100%
Bloqueio de Números			67%
Base de Dados			67%
Bloqueio de Fraudes			100%
Responsável Designado	46%	50%	100%
Estratégia Multissectorial	0%	0%	50%
Tipos de Fraudes	31%	25%	67%
Média	20%	25%	73%

Tabela 7: Indicadores de Fraude

De forma detalhada seguem as constatações identificadas no processo da gestão de fraudes.

1. Serviço de Denúncia

As MNO registam 33% de implementação de canais formais de denúncia de fraudes, evidenciando maior maturidade institucional, seguidos pelos operadores de TV (25%) e os ISP (15%), evidenciando lacunas significativas neste ultimo segmento.

2. Comunicação com o Regulador

Cerca de 100% das MNO mantêm comunicação em tempo real com a Autoridade Reguladora, contra 25% dos operadores de TV e 8% os ISP, evidenciando vulnerabilidades nos sectores menos desenvolvidos.

3. Bloqueio de Números

Relativamente ao bloqueio de números suspeitos, esta acção é aplicável apenas às MNO, que implementaram mecanismos para o efeito com uma eficácia de cerca de 67%. Os restantes subsectores não dispõem deste tipo de serviço.

4. Base de Dados

Esta medida e respectivo sistema são exclusivos das MNO, com 67% das operadoras a reportarem a utilização de bases de dados estruturadas para identificação e gestão de terminais associados a fraudes. Nenhum dos outros subsectores dispõe de soluções equivalentes, o que evidencia uma falha crítica na prevenção e monitorização de comportamentos maliciosos.

5. Bloqueio de Fraudes

As MNO realizam, de forma sistemática, o bloqueio diário de terminais e números fraudulentos, com 100% dos casos reportados, demonstrando um elevado grau de operacionalização dos seus mecanismos de resposta. Já os subsectores de TV e ISP não adoptam esta prática nos seus dispositivos, o que pode originar janelas de vulnerabilidade prolongadas.

6. Responsável Designado

Todas as MNO (100%) dispõem de equipas especializadas dedicadas à gestão de fraudes. No subsector da TV, este valor desce para 50%, enquanto entre os ISP apenas 46% contam com responsáveis designados, o que compromete a eficácia das acções de mitigação e resposta.

7. Estratégia Multissectorial

Apenas 50% das MNO participam em iniciativas de colaboração com outros sectores. Os ISP e as TV reportam 0%, revelando ausência total de cooperação intersectorial, um factor que limita a eficácia da resposta colectiva.

8. Tipos de Fraudes

As MNO registam uma incidência de 67%, confirmando-se como o alvo preferencial das actividades fraudulentas. Os ISP indicam 31%, e a TV 25%, sugerindo menor exposição, mas também potencial subnotificação ou falta de capacidade de detecção.

3.2.3. Conclusão

Com base na análise dos indicadores apresentados, conclui-se que o sector das telecomunicações em Moçambique ainda se encontra numa fase inicial de maturidade no que respeita à gestão de fraudes, com fortes assimetrias entre os subsectores. As MNO evidenciam uma estrutura mais robusta, com mecanismos de detecção e resposta eficazes, canais de comunicação activos com o Regulador e equipas especializadas, o que sustenta o seu desempenho superior nesta dimensão.

Por outro lado, os ISP e as TV revelam fragilidades significativas, sobretudo na ausência de processos estruturados, baixa articulação institucional e inexistência de sistemas automatizados de monitorização e bloqueio. A falta de estratégias multissectoriais e a reduzida presença de canais formais de denúncia dificultam ainda mais a eficácia das acções de prevenção e mitigação.

Face a este cenário, torna-se imperativo reforçar as capacidades dos subsectores menos maduros, promovendo a padronização de práticas, o investimento em tecnologias antifraude e o estreitamento da cooperação com o Regulador e demais actores do ecossistema. A harmonização dos mecanismos de resposta é essencial para garantir uma postura coordenada, proactiva e resiliente face ao crescente risco de actividades fraudulentas no sector.

3.2.4. Recomendações da Secção

Com base nos resultados obtidos e nas fragilidades identificadas ao longo da análise, apresenta-se, a seguir, um conjunto de recomendações estratégicas destinadas a fortalecer a resposta do sector às fraudes, promovendo maior uniformidade, eficiência e cooperação entre os operadores e a Autoridade Reguladora.

1. Reforço da Capacidade de Resposta

- Criação de equipas dedicadas à gestão de fraudes em todas as operadoras, com formação técnica especializada.
- Implementação de sistemas automatizados de bloqueio, com base nas boas práticas já aplicadas pelas MNO.
- Desenvolvimento de bases de dados partilhadas de terminais suspeitos, com acesso regulado e supervisionado pela Autoridade Reguladora.

2. Melhoria da Articulação com a Autoridade Reguladora

- Estabelecimento da obrigatoriedade de comunicação em tempo real para todos os subsectores, com mecanismos de penalização em caso de incumprimento.
- Submissão de relatórios periódicos normalizados, com registo de fraudes detectadas e medidas aplicadas, facilitando a análise comparativa.

3. Promoção da Cooperação Multissectorial

- Criação de uma plataforma central de partilha de informação, envolvendo MNO, ISP, TV e entidades financeiras.
- Lançamento de campanhas conjuntas de sensibilização dirigidas ao público, com foco em fraudes recorrentes como SIM Swap e phishing.

4. Investimento em Inovação e Detecção Proactiva

- Adopção de soluções baseadas em inteligência artificial para detecção em tempo real de padrões suspeitos.
- Realização de auditorias de segurança regulares, com definição de metas progressivas de melhoria.

5. Harmonização Legal e Regulamentar

- Revisão do quadro normativo para estabelecer obrigações mínimas em matéria de prevenção, como o bloqueio automático após denúncia.
- Criação de incentivos fiscais para operadoras que invistam em tecnologias de prevenção e detecção de fraude.

3.3. Protecção de Dados e Privacidade

A protecção de dados pessoais e a garantia da privacidade dos utilizadores constituem pilares fundamentais para a confiança nos serviços de telecomunicações. Neste contexto, foram analisados 8 indicadores-chave, com o propósito de avaliar o grau de compromisso dos operadores com a segurança e integridade da informação dos consumidores.

A análise incluiu a revisão das políticas internas de protecção de dados, a verificação da conformidade com os regulamentos aplicáveis, bem como a avaliação das medidas de segurança implementadas e dos procedimentos de recolha, tratamento e armazenamento de dados.

3.3.1. Apreciação Geral

No domínio da protecção de dados e privacidade, o sector das telecomunicações alcançou uma pontuação média de 61%, o que corresponde a um nível de maturidade avançado, embora situado ainda no limite inferior da faixa intermédia. Este resultado reflecte a existência de estruturas operacionais básicas, com políticas formalizadas, procedimentos de segurança estabelecidos e sistemas de controlo parcialmente implementados.

O gráfico seguinte demonstra a distribuição do posicionamento dos subsectores quanto a esta dimensão.

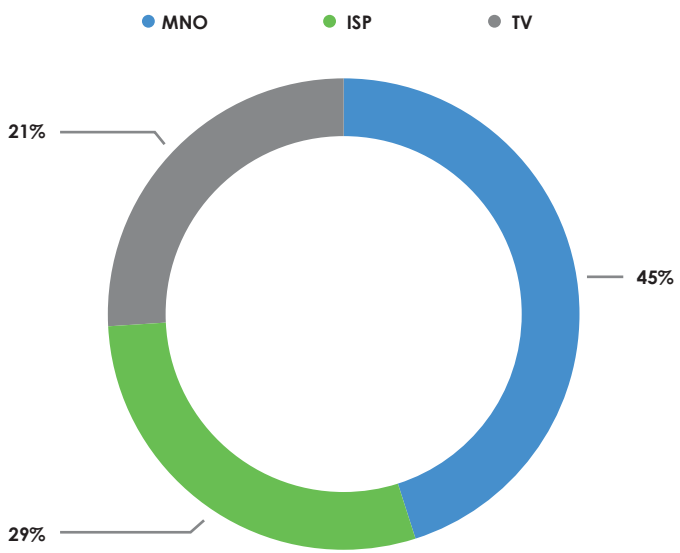


Gráfico 4: Nível de Maturidade Sectorial na Protecção de dados

A análise por segmento revela disparidades marcantes no desempenho em matéria de protecção de dados e privacidade. As MNO lideram com 45% de maturidade sectorial nesta dimensão, resultado sustentado por controlos técnicos robustos, auditorias regulares e uma cultura organizacional consolidada em torno da segurança da informação.

Os ISP apresentam uma percentagem de 29%, marcada por vulnerabilidades críticas, que evidenciam a necessidade de padronizar práticas, automatizar controlos e reforçar a capacitação interna. Já o segmento de TV, com 26%, embora disponha de políticas formalmente estruturadas, enfrenta dificuldades na sua aplicação prática, agravadas por baixos níveis de investimento em formação e ausência de mecanismos de verificação contínua, o que compromete a eficácia das medidas adoptadas.

3.3.2. Apreciação detalhada por Subsector

Nesta subsecção apresentam-se os indicadores relacionados com a protecção de dados e privacidade nos três subsectores das telecomunicações, com o objectivo de oferecer uma visão comparativa detalhada sobre os níveis de maturidade, práticas implementadas e as áreas críticas que carecem de reforço, conforme é apresentado na tabela abaixo.

Indicadores	ISP	TV	MNO
Protecção de Dados	45%	38%	83%
Conformidade Regulamentar	40%	35%	73%
Gestão de Incidentes	42%	40%	83%
Controlos de Acesso	38%	33%	67%
Formação Consciencialização	48%	45%	80%
Armazenamento de Dados	85%	75%	100%
Segurança em Cloud	35%	25%	70%
Políticas Documentadas	92%	88%	100%
Média	53%	47%	82%

Tabela 8: Indicadores de Protecção de Dados

De forma detalhada seguem as constatações identificadas em relação a secção de protecção de dados:

1. Protecção de Dados

As MNO lideram com 83%, destacando-se pelos mecanismos de encriptação, controlo de acessos e monitoria contínua, todos bem implementados. Seguem-se os ISP, com 45%, que apresentam uma aplicação inconsistente dessas medidas, enquanto as operadoras de TV registam 38%, evidenciando fragilidades na protecção de dados sensíveis.

2. Conformidade Regulamentar

As MNO lideram com 73%, destacando-se pela realização de auditorias, formação contínua e apoio técnico especializado. Os ISP seguem com 40%, apresentando práticas ainda incipientes, enquanto as operadoras de TV, com 35%, requerem acções urgentes para reforçar a conformidade.

3. Gestão de Incidentes

As MNO apresentam um nível de maturidade de 83%, evidenciando forte capacidade de res-

posta sustentada por planos formais e equipas devidamente treinadas. Em contrapartida, os ISP (42%) e o segmento da TV (40%) operam com processos frágeis, aumentando o risco de impactos operacionais e reputacionais em caso de incidentes.

4. Controlos de Acesso

A autenticação multifactorial é utilizada por 67% das MNO, garantindo maior protecção nos acessos. Nos ISP, a adopção é de 38%, reflectindo uma aplicação inconsistente, enquanto as TV, com apenas 33%, permanecem vulneráveis a acessos não autorizados.

5. Formação e Consciencialização

As MNO demonstram forte compromisso com a formação contínua (80%), incluindo simulações práticas como ataques de *phishing*. Já os ISP (48%) e as operadoras de TV (45%) realizam formações mais genéricas e esporádicas. Apenas 15% dos ISP integram exercícios práticos, limitando a eficácia da preparação dos seus colaboradores.

6. Armazenamento de Dados

As MNO asseguram 100% de localização nacional dos dados e utilizam cloud internacional com plena conformidade legal. Os ISP mantém 85% dos dados localmente, enquanto a TV apresenta 75% de dados nacionais e 25% em *cloud*.

7. Segurança em *Cloud*

Mais uma vez, as MNO lideram com 70% de maturidade, recorrendo a práticas como encriptação ponta-a-ponta e backups seguros. Os ISP apresentam 35%, e as TV, com apenas 25%, evidenciam atraso na adopção de tecnologias cloud seguras e em conformidade legal.

8. Políticas Documentadas

No que diz respeito à existência de políticas documentadas, as MNO apresentam uma taxa de conformidade de 100%, seguidas pelos ISP com 92% e pela TV com 88%, evidenciando uma boa adesão formal, embora persistam desafios na implementação prática, sobretudo nos subsectores com menor maturidade operacional.

3.3.3. Conclusão

O sector das telecomunicações em Moçambique revelam progressos significativos no domínio da protecção de dados e privacidade, com uma média global de maturidade de 61%. Contudo, persistem assimetrias relevantes entre os diferentes subsectores. As MNO destacam-se

pela adopção de práticas sólidas e sistematizadas, reflectindo um compromisso firme com a segurança da informação.

Em contrapartida, os ISP e, as TV, revelam fragilidades estruturais que comprometem a eficácia das medidas adoptadas, o que evidencia a necessidade de reforçar a implementação prática de políticas existentes, investir em capacitação contínua e garantir mecanismos eficazes de monitorização e conformidade.

3.3.4. Recomendações

A avaliação do nível de maturidade na protecção de dados revela um cenário de risco moderado, caracterizado pela existência de estruturas básicas implementadas, mas ainda com falhas significativas na aplicação prática, na verificação contínua e na formação especializada. Face a este contexto, apresentam-se as seguintes recomendações prioritárias, para reforçar a resiliência e garantir conformidade legal e técnica no tratamento de dados:

1. Reforçar a Implementação Técnica

- Adoptar mecanismos obrigatórios de autenticação multifactorial e controlo de acessos em todos os operadores.
- Expandir o uso de encriptação avançada e soluções de monitoria contínua, especialmente entre os ISP e a TV.
- Padronizar os requisitos de segurança em ambientes cloud, garantindo conformidade jurídica e técnica.

2. Fortalecer a Conformidade Regulamentar

- Implementar auditorias internas regulares nos ISP e TV, acompanhadas de planos de acção para correcção de não conformidades.
- Reforçar o reporte periódico obrigatório sobre medidas de protecção de dados e actualização das políticas.

3. Investir em Formação e Capacitação

- Estabelecer programas contínuos de formação e simulações práticas (ex: phishing) em todos os operadores.
- Promover certificações técnicas para equipas responsáveis por segurança e privacidade.

4. Promover a Cooperação Sectorial

- Criar linhas orientadoras comuns para protecção de dados, aplicáveis a todos os subsectores, sob coordenação do Regulador.
- Estimular plataformas de partilha de boas práticas e experiências sobre incidentes de privacidade entre operadores.

***5.* Monitorar e Avaliar**

- Definir indicadores de desempenho obrigatórios relacionados com a protecção de dados, e com acompanhamento regular por parte do Regulador.
- Estabelecer metas progressivas de maturidade, com incentivos para operadores que atinjam níveis mais elevados de conformidade e segurança.

3.4. Resiliência da Rede de Telecomunicações

A resiliência das redes constitui um elemento fundamental para assegurar a continuidade dos serviços de telecomunicações, mesmo perante falhas técnicas, incidentes operacionais ou ataques cibernéticos . Esta secção, composta por dez (10) indicadores, teve como objectivo avaliar a capacidade dos operadores e prestadores de serviços públicos de telecomunicações em matérias de segurança e resiliência.

A análise centrou-se na avaliação da eficácia dos planos de continuidade e recuperação, dos mecanismos de redundância implementados e as medidas preventivas adoptadas para mitigar falhas e maximizar a disponibilidade operacional das redes.

3.4.1. Apreciação Geral

O sector das telecomunicações apresenta um nível de maturidade intermédio em matéria resiliência (63%), evidenciando a existência de capacidades básicas de gestão de riscos, continuidade operacional e resposta a incidentes.

Apesar deste desempenho reflectir progressos importantes, persistem disparidades significativas entre os diferentes subsectores, o que exige a implementação de intervenções específicas e direccionadas para garantir uma resiliência homogénea no sector.

O gráfico seguinte demonstra a distribuição do posicionamento dos subsectores quanto a esta dimensão.

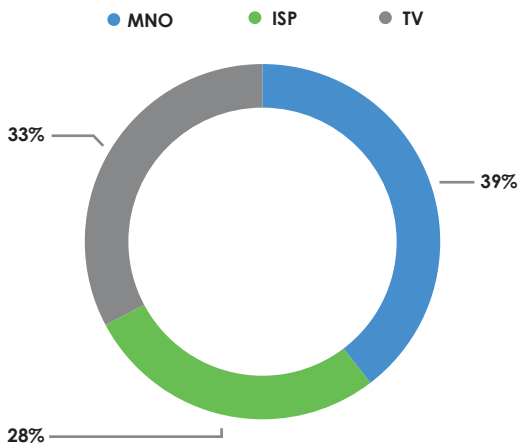


Gráfico 5: Nível de Maturidade Sectorial na Resiliência

A análise comparativa dos subsectores revela diferencas significativas no nível de maturidade em matéria de resiliência. As lideramMNO com um nível de maturidade de 39%, resultado de uma abordagem técnica consolidada, que integra sistemas de redundância eficazes, protocolos de gestão de falhas bem definidos e capacidade de recuperação.

Os operadores de TV seguem com 33%, evidenciando esforços consistentes na monitoria da rede, contudo, ainda apresentam lacunas relevantes, nomeadamente a ausência de planos de contingência devidamente formalizados e a execução de testes de recuperação.

Por sua vez, os ISP, registam um nível de maturidade mais baixo, com 28%, evidenciando fragilidades de caracter operacional e regulamentar. Estas fragilidades são agravadas pela utilização de processos desactualizados e pela limitação com o regulador, o que aumenta a a sua exposição a interrupções críticas.

3.4.2. Apreciação Detalhada por Subsector

De forma detalhada, seguem-se as principais constatações relativas aos indicadores de resiliência observadas em cada subsector, permitindo uma análise comparativa entre estes. Esta apreciação evidencia, igualmente, o grau de implementação das práticas essenciais para garantir continuidade de serviços, bem como as principais fragilidades operacionais e estruturais que comprometem a robustez das redes, a tabela abaixo apresenta a descrição desta secção por subsector.

Indicadores	ISP	TV	MNO
Estratégias de Resiliência	48%	45%	80%
Activação de Redundância	85%	100%	100%
Controlos contra Ameaças	48%	60%	80%
Plano Documentado	69%	50%	67%
Monitoria Proactivo	48%	63%	67%
Protecção contra Desastres	48%	60%	73%
Tempo de Reporte	69%	100%	100%
Partilha de Dados	19%	25%	67%
Planificação de Escalabilidade	48%	50%	60%
Resposta a Incidentes	48%	65%	60%
Média	53%	62%	75%

Tabela 9: Indicadores de Resiliência

De forma detalhada seguem as constatações identificadas na secção segurança e resiliência das redes:

1. Estratégias de Resiliência

As MNO registam um nível de implementação de estratégias formais de resiliência de 80%, demonstrando uma preparação robusta para garantir a continuidade dos serviços. Em contra-partida, os ISP, com (48%) e as TV, com (45%), apresentam níveis significativamente inferiores, o que revela limitações significativas na sua capacidade de resposta em cenários de falha.

2. Activação de Redundância

As MNO e as TV alcançam 100% de conformidade na activação de redundancia, assegurando mecanismos que permite activação imediata de sistemas redundantes. Os ISP, com (85%), embora apresentem desempenho próximo, ainda possuem pontos únicos de falha em 15% dos casos, comprometendo a disponibilidade contínua dos serviços.

3. Controlos Contra Ameaças

As MNO lideram com 80% de implementação de medidas de protecção contra ameaças físicas e digitais, evidenciando uma abordagem solida e abrangente. As TV apresentam 60%, adoptando práticas de forma parcial, enquanto os ISP, com 48%, revelam falhas críticas, com quase metade dos seus sistemas sem mecanismos eficazes de mitigação.

4. Plano Documentado

Os ISP lideram com (69%) de implementação de planos documentados, seguidos pelas MNO

(67%), enquanto a TV (50%), revelando baixa formalização, o que compromete a eficácia da resposta coordenada em situações críticas.

5. Monitoria Proactiva

As MNO lideram (67%) de implementação de monitoria continua, seguidas pelas TV (63%), demonstrando níveis razoáveis de monitoria contínua da rede. Os ISP (48%), encontram-se em situação mais vulnerável, refletindo lacunas na detecção precoce de problemas, o que pode prolongar o tempo de inactividade em caso de incidente.

6. Protecção Contra Desastres

As MNO lideram (73%), mantendo níveis elevados de resiliência física, suportados por estruturas reforçadas e planos para resposta a eventos climáticos extremos. As TV registam (60%), enquanto que os ISP apresentam (48%), evidenciando maior exposição e a necessidade de reforço nas medidas de contingência.

7. Tempo de Reporte

As MNO e a TV lideram com 100% de conformidade, assegurando a comunicação tempestiva de falhas e incidentes, enquanto os ISP apresentam (69%), evidenciando maior exposição e necessidade de reforço das medidas, uma vez que cerca de um terço dos operadores a reportar fora dos prazos estabelecidos.

8. Partilha de Dados

As MNO lideram com (67%), evidenciando uma prática consolidada de partilha de informação, embora ainda exista margem para melhoria quanto à frequência e profundidade dos dados partilhados. As TV registam (25%), enquanto os ISP apresentam apenas 19%, o que dificulta a ação regulatória e a resposta sectorial coordenada.

9. Planificação de Escalabilidade

As MNO lideram com (60%), evidenciando alguma preparação para lidar com picos de procura. Seguem-se as empresas de televisão, com (50%), e os ISP, com (48%), revelando fragilidades na planificação. A ausência de estratégias robustas para expansão e adaptação das redes pode comprometer a resiliência futura, sobretudo em situações de emergência.

10. Resposta à Incidentes

As TV lideram com (65%), apresentando o melhor desempenho nesta dimensão, seguidas

de MNO com (60%) e ISP, com (48%). A baixa capacidade de resposta entre os ISP denuncia limitações operacionais e técnicas que podem amplificar os impactos de falhas ou ataques.

3.4.3. Conclusão

A análise da dimensão de resiliência evidencia progressos relevantes no sector das telecomunicações, mas também sublinha a existência de disparidades significativas entre os subsectores. As MNO mantêm a liderança com práticas mais maduras e estruturadas, beneficiando de sistemas robustos e planos bem definidos, enquanto as TV demonstram avanços pontuais, sobretudo na resposta a incidentes e monitorização contínua, embora careça de formalização em áreas críticas. Os ISP permanecem como o grupo mais vulnerável, com deficiências notórias em quase todos os indicadores avaliados, desde a partilha de dados até à protecção contra ameaças.

Torna-se, assim, imperativo reforçar a resiliência de forma integrada e coordenada, promovendo a actualização de processos, o desenvolvimento de capacidades técnicas e a uniformização das práticas entre operadores. A consolidação de estratégias formais de continuidade e a melhoria da articulação com o regulador devem ser prioridades para garantir que todo o sector esteja preparado para enfrentar disrupções com eficácia, minimizando riscos operacionais e assegurando a confiança dos utilizadores.

3.4.4. Recomendações

O desempenho do sector das telecomunicações em termos de resiliência operacional e continuidade de serviços evidencia progressos em áreas como a monitoria proactiva e a implementação de redundância básica. Contudo, existem lacunas críticas em infra-estruturas, auditorias, resposta a incidentes e conformidade regulatória. A diversidade de níveis de maturidade entre subsectores exige medidas diferenciadas, mas sempre alinhadas com um objectivo comum: garantir a robustez, a disponibilidade e a capacidade de recuperação eficaz face a falhas técnicas, desastres naturais ou ciberataques.

1. Formalização de Planos e Estratégias

- Todos os operadores devem manter planos de continuidade e recuperação documentados, revistos periodicamente e alinhados com os requisitos regulatórios.
- As TV e os ISP devem priorizar a criação e validação de planos formais, com simulações práticas de activação.

2. Reforço da Redundância e Monitorização

- Os ISP devem eliminar os pontos únicos de falha, garantindo sistemas de redundância

total em todos os nós críticos.
- Ampliar o uso de monitorização proactiva e alertas automatizados, especialmente nos segmentos com menor maturidade.

3. Gestão de Incidentes e Partilha de Informação

- Implementar protocolos padronizados de resposta a incidentes, com registos de acções, tempos de resposta e indicadores de impacto.
- Aumentar os níveis de partilha de dados operacionais e técnicos com a autoridade reguladora, sobretudo por parte dos ISP e das TV.

4. Planeamento de Escalabilidade

- Desenvolver planos específicos para adaptação da rede a aumentos súbitos de carga ou expansão territorial, garantindo continuidade mesmo sob pressão elevada.

5. Formação e Simulações

- Realizar simulações regulares de falhas ou ataques para testar os mecanismos de resposta e recuperação.
- Integrar as equipas operacionais e de segurança nos exercícios, garantindo a coordenação multidisciplinar.

6. Diferenciação por Subsector

- As MNO devem consolidar as boas práticas e reforçar planos de escalabilidade.
- As TV devem investir na formalização de processos, documentação e partilha de dados.
- Os ISP devem implementar medidas estruturantes de base, com foco em conformidade, redundância e resposta operacional.

3.5. Controlos e Medidas de Segurança

A segurança das redes e sistemas constitui um dos pilares essenciais para a fiabilidade e resiliência do sector das telecomunicações. Nesta secção, foram analisados dez (10) indicadores-chave, com o objectivo de avaliar as práticas, procedimentos e sistemas implementados para proteger infra-estruturas críticas contra ameaças e vulnerabilidades.

A análise centrou-se na verificação dos controlos de segurança existentes, na revisão das políticas e procedimentos operacionais adoptados, na avaliação das medidas de protecção

de dados aplicadas e na eficácia dos sistemas de monitorização e resposta a incidentes.

3.5.1. Apreciação Geral

O sector das telecomunicações apresenta um nível optimizado de maturidade em matéria de segurança da informação, com uma pontuação média global de 86% nas medidas de controlo avaliadas. Este desempenho reflecte a existência de políticas robustas, sistemas eficazes de autenticação, e mecanismos regulares de auditoria e monitorização, colocando esta dimensão entre as mais consolidadas do sector.

Contudo, a análise segmentada revela diferenças relevantes entre os subsectores, com níveis distintos de evolução e consolidação das práticas de segurança, conforme ilustra o gráfico abaixo.

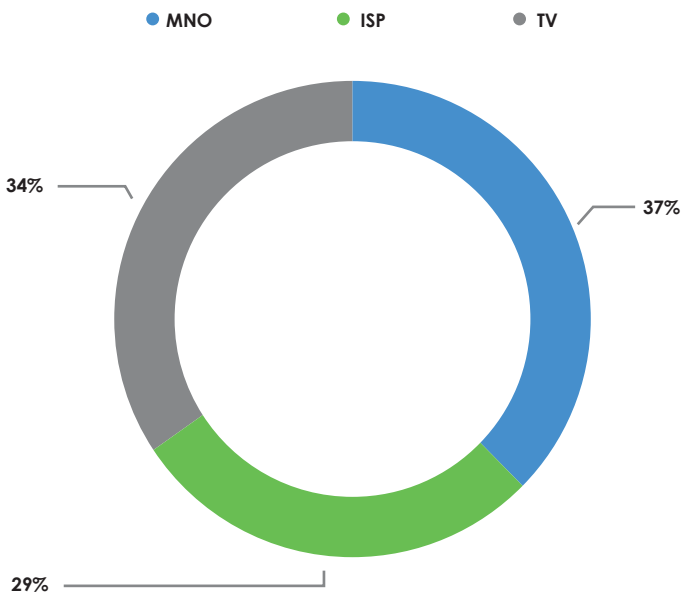


Gráfico 6: Nível de Maturidade Sectorial dos Controlos e Medidas de Segurança

Na dimensão de Controlos e Medidas de Segurança, as MNO assumem a liderança com 39% de maturidade, demonstrando uma abordagem sólida baseada em encriptação robusta, controlo de acessos eficaz e mecanismos automatizados de resposta a incidentes.

As TV seguem com 33%, apresentando políticas bem estruturadas e sistemas de protecção minimamente consolidados. Apesar disso, enfrentam fragilidades na gestão de fornecedores e terceiros, uma área em que a falta de critérios uniformes e a ausência de controlos mais exigentes comprometem a eficácia global das medidas aplicadas.

Por sua vez, os ISP registam 28% de maturidade, ocupando a terceira posição. Este segmento revela debilidades mais acentuadas, principalmente no que toca à conformidade regulatória, segurança em ambientes de cloud e à comunicação interna das políticas de segurança.

3.5.2. Apreciação Detalhada por Subsector

De forma detalhada, seguem-se as principais constatações relativas aos indicadores de controlos e medidas de segurança, com uma análise comparativa entre os três subsectores. Esta análise permite identificar os níveis de implementação das práticas essenciais para garantir continuidade de serviços, bem como as principais lacunas operacionais e estruturais que afectam a robustez das redes.

Indicadores	ISP	TV	MNO
Política Documentada	77%	100%	100%
Comunicação da Política	69%	100%	100%
Inventário Actualizado	81%	88%	100%
Mecanismos de Activos	81%	88%	100%
Política de Controlo	89%	100%	100%
Segregação de Redes	73%	88%	100%
Cifragem de Dados	73%	88%	100%
Processo de resposta	58%	63%	83%
Controlos para fornecedores	69%	88%	100%
Avaliação de Controlos	77%	100%	100%
Média	75%	90%	98%

Tabela 10: Indicadores de Controlos e Medidas de Segurança

De forma detalhada seguem as constatações em relação a secção:

1. Política Documentada

As MNO e as TV apresentam 100% de conformidade, demonstrando a existência de políticas de segurança bem estabelecidas e formalmente aprovadas. Os ISP, com 77%, revelam lacunas que podem comprometer a definição clara de responsabilidades e aplicação consistente das práticas de segurança.

2. Comunicação da Política

As MNO e as TV comunicam integralmente as suas políticas de segurança atingindo (100%) de conformidade, por sua vez apenas (69%) os ISP, comunicam as politicas de forma adequada, comprometendo a disseminação efectiva disseminação das orientações internas e pode dificultando a sua aplicação consistente.

3. Inventário Actualizado

As MNO lideram (100%) de conformidade, garantindo um controlo rigoroso sobre activos críticos. As TV apresentam (88%), enquanto os ISP, com 81%, demonstram algum nível de controlo, mas ainda com margem de melhoria na rastreabilidade de equipamentos e sistemas.

4. Mecanismos de Activos

As MNO com (100%) de implementação, evidenciando adopção de práticas preventivas solidas contra a perda de activos. As TV atingem 88%, enquanto os ISP, registam (81%), evidenciando a necessidade de reforçar medidas como rastreabilidade e backups físicos e lógicos.

5. Política de Controlo

As TV e MNO registam (100%) de conformidade, possuindo políticas claras de controlo de acessos, enquanto os ISP, com (89%), evidenciando desempenho próximo, mas ainda enfrentam desafios na uniformização e no controlo de privilégios excessivos.

6. Segregação de Redes

As MNO lideram com (100%) de conformidade, demonstrando uma abordagem avançada

à protecção das suas infra-estruturas, seguido das TV, com (88%), mantendo boas práticas, enquanto que os ISP, com (73%), apresentam riscos acrescidos de propagação lateral de ataques, em caso de intrusões.

7. Cifragem de Dados

As MNO lideraram com (100%), assegurando a confidencialidade dos dados durante a sua transmissão. As TV registam (88%), enquanto os ISP, com (73%), afigura-se necessário investir em encriptação mais robusta, especialmente em canais sensíveis.

8. Processo de Resposta

As MNO lideram com 83%, dispondo de processos formais para resposta a incidentes, seguidas da TV com (63%), enquanto os ISP, com 58%, demonstrando graves lacunas na capacidade de resposta organizada e tempestiva a eventos de segurança.

9. Controlos para Fornecedores

As MNO lideram com (100%) de cobertura, estabelecendo requisitos claros e rigorosos para fornecedores e terceiros. As TV registam (88%), enquanto os ISP apenas (69%), evidenciando fragilidades contratuais e operacionais significativas, particularmente em contextos de *outsourcing* e serviços em *cloud*.

10. Avaliação de Controlos

As MNO e as TV atingem (100%) do nível de maturidade, evidenciando uma cultura consolidada de melhoria contínua. Os ISP, com 77%, embora acima da média, necessitam de evoluir para práticas mais sistemáticas de auditoria e reavaliação dos controlos implementados.

3.5.3. Conclusão

A análise da dimensão Controlos e Medidas de Segurança mostra um desempenho global elevado no sector das telecomunicações (86%), mas com diferenças relevantes entre os subsectores.

As MNO lideram com práticas consolidadas em encriptação, controlo de acessos e avaliação contínua dos controlos, demonstrando uma maturidade operacional elevada. As TV apresentam bons resultados em vários indicadores, mas revelam fragilidades na gestão de fornecedores e na resposta a incidentes. Já os ISP enfrentam desafios mais acentuados, com lacunas na comunicação interna das políticas, na protecção em ambientes terceirizados e na formalização de processos de resposta.

Apesar dos avanços, torna-se essencial reforçar os mecanismos de controlo, especialmente entre os ISP e as TV, promovendo padronização, formação contínua e maior automatização das medidas de segurança.

3.5.4. Recomendações

A segurança da informação tornou-se um eixo crítico para a continuidade e confiança nas infraestruturas de telecomunicações. Apesar de progressos em várias frentes, persistem assimetrias entre os operadores, especialmente no segmento ISP. O conjunto de recomendações a seguir apresentado visa uniformizar práticas, elevar o nível de maturidade do sector e garantir alinhamento com padrões internacionais.

1. Reforço das Capacidades Técnicas

- Garantir a implementação obrigatória de processos formais de resposta a incidentes em todos os operadores.
- Aumentar a adopção de encriptação robusta de dados em movimento, alinhando com as práticas das MNO.
- Desenvolver e actualizar inventários de activos com mecanismos automatizados de detecção de anomálias.

2. Padronização e Avaliação Contínua de Controlos

- Estabelecer critérios mínimos obrigatórios de controlo de acessos e segregação de redes em todos os subsectores.
- Promover ciclos regulares de avaliação da eficácia dos controlos, incluindo auditorias internas e externas.
- Estimular o uso de indicadores de desempenho em segurança operacional, com metas claras de melhoria.

3. Gestão Segura de Terceiros e Fornecedores

- Definir requisitos contratuais padronizados para fornecedores, incluindo cláusulas de segurança e *compliance*.
- Reforçar o controlo sobre serviços externalizados, com especial atenção a fornecedores de *cloud computing*.

4. Comunicação e Sensibilização Interna

- Garantir a comunicação eficaz das políticas de segurança a todos os colaboradores, com métricas de acompanhamento.
- Promover campanhas de consciencialização regulares sobre os riscos e procedimentos de segurança, especialmente nos ISP.

5. Cooperação Sectorial e Supervisão Reguladora

- Criar mecanismos de partilha de boas práticas de segurança entre operadores.
- Incentivar a adopção voluntária de normas internacionais de cibersegurança, como a ISO/IEC 27001, através de programas de reconhecimento e certificação.
- Reforçar o acompanhamento por parte da Autoridade Reguladora, com a avaliação periódica da evolução dos indicadores.

3.6. Preparação e Resposta a Incidentes

A presente secção avaliou o nível de preparação e capacidade de resposta das organizações perante incidentes de segurança da informação, com base nas normas ISO/IEC 27001, NIST CSF e COBIT.

A preparação para incidentes envolve a existência de políticas, procedimentos, equipas e ferramentas que permitam à organização detectar, gerir e recuperar eficazmente de ocorrências que comprometam a segurança da informação. Este processo é essencial para assegurar a resiliência operacional e a continuidade dos serviços.

A análise teve como objectivo identificar o grau de maturidade dos mecanismos existentes, avaliando o alinhamento com os níveis de segurança, contingência e continuidade de negócio ajustados ao perfil de cada entidade.

3.6.1. Apreciação Geral

O sector das telecomunicações apresenta um nível de maturidade avançado (61%) no que se refere à preparação e resposta a incidentes, evidenciando a existência de planos de contingência básicos, procedimentos operacionais definidos e uma crescente preocupação com a continuidade dos serviços em situações críticas.

No entanto, esta média sectorial oculta assimetrias significativas entre os subsectores, que comprometem uma resposta coordenada e eficaz em todo o ecossistema, conforme é apresentado no gráfico abaixo:

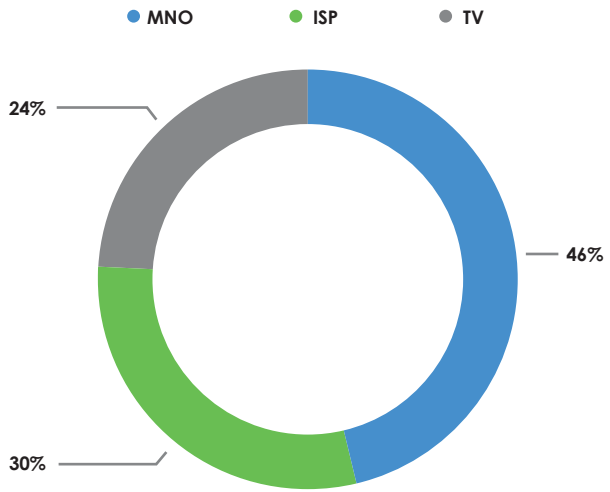


Gráfico 7: Nível de Maturidade de Preparação e Resposta a Incidentes

Na dimensão de Preparação e Resposta a Incidentes, as MNO apresentam o desempenho mais elevado, com 46% da maturidade global, evidenciando processos robustos, equipas especializadas, monitorização contínua e planos bem definidos que asseguram uma resposta rápida e eficaz a eventos críticos.

Os ISP, com 30%, posicionam-se num nível intermédio, mas revelam grandes disparidades internas especialmente quanto à qualificação dos recursos humanos e à ausência de planos formais de resposta, o que pode comprometer a actuação em situações mais complexas.

As TV, com 24%, registam o desempenho mais baixo, marcado pela falta de equipas técnicas dedicadas, baixa formalização de procedimentos e fraca capacidade de reacção imediata, factores que colocam em risco a fiabilidade dos seus serviços em caso de incidentes.

3.6.2. Apreciação Detalhada por Subsector

De forma detalhada, seguem-se as principais constatações relativas aos indicadores de controlos e medidas de segurança, com uma análise comparativa entre os três subsectores. Esta análise permite identificar os níveis de implementação das práticas essenciais para garantir a continuidade de serviços, bem como as principais lacunas operacionais e estruturais que afectam a robustez das redes.

Indicadores	ISP	TV	MNO
Equipa Dedicada	46%	50%	67%
Plano de Resposta	58%	50%	83%
Sistemas de Monitoria	62%	50%	100%
Uso de Logs	50%	25%	83%
Análise de Incidentes	58%	50%	83%
Planos de Contingência	58%	50%	83%
Comunicação	42%	25%	83%
Auditoria	62%	50%	100%
Média	55%	44%	85%

Tabela 11: Indicadores de Preparação e Resposta a Incidentes

De forma detalhada seguem as constatações em relação à secção:

1. Equipa Dedicada

As MNO lideram com (67%), dispondo de equipas especializadas para a gestão de ciberincidentes, seguidas pela TV com (50%), enquanto os ISP, com (46%),evidenciando carências estruturais, uma vez que mais de metade não possui equipas dedicadas à gestão de incidentes de segurança.

2. Plano de Resposta

As MNO destacam-se com (83%) dos operadores a manterem planos de resposta actualizados e operacionais, enquanto, os ISP e as TV registam entre 50% e 58%, evidenciando que osplanos são frequentemente desactualizados ou pouco funcionais, comprometendo a eficácia e a prontidão da resposta.

3. Sistemas de Monitoria

As MNO implementam na totalidade (100%), os sistemas de detecção de intrusões (IDS/IPS), enquanto os ISP e as TV têm níveis mais baixos (62% e 50%, respectivamente), o que pode deixar janelas de detecção abertas a ameaças persistentes, especialmente em redes críticas.

4. Uso de Logs

As MNO lideram com (83%), evidenciando capacidade consolidada de correlação e análise contínua de eventos de segurança. Seguem-se os ISP, com (50%), enquanto as empresas de te-

levisão apresentam apenas (25%), demonstrando níveis de implementação ainda insuficientes, o que limita a visibilidade sobre padrões anómalos e dificulta investigações forenses.

5. Análise de Incidentes

As MNO mantém um desempenho elevado (83%) com procedimentos bem definidos para análise de causas de incidentes. Os ISP (58%) e a TV (50%) mostram abordagens menos estruturadas, limitando a prevenção de recorrências e a melhoria contínua.

6. Planos de Contingência

As MNO lideram com (83%) de implementação de planos de contingência robustos e actualizados. Já os ISP (58%) e a TV (50%) apresentam lacunas relevantes, com planos pouco ajustados aos riscos críticos do sector, como protecção de dados e continuidade operacional.

7. Comunicação

As MNO lideram com (83%), destacando-se pelas boas práticas que asseguram notificações céleres e uma articulação eficiente em contextos de crise. Seguem-se os ISP, com (42%), e as TV, com (25%), que revelam fragilidades significativas na comunicação com o regulador e outras partes interessadas, comprometendo a eficácia da resposta coordenada.

8. Auditoria

As MNO lideram com (100%) de cobertura, evidenciando um forte compromisso com a validação externa da eficácia dos seus mecanismos de resposta, seguem-se os ISP com (62%) e as TV com (50%), o que sugere que as auditorias externas ainda não são uma prática generalizada nestes subsectores.

3.6.3. Conclusão

A análise da dimensão de Preparação e Resposta a Incidentes revela que, apesar do sector das telecomunicações apresentar um nível de maturidade avançado (61%), subsistem desigualdades entre os subsectores.

As MNO destacam-se como referência, com mecanismos estruturados e equipas dedicadas, enquanto os ISP e as TV enfrentam fragilidades na formalização de planos, na especialização técnica e na comunicação com o regulador.

Para garantir uma resposta colectiva eficaz, torna-se essencial investir em recursos humanos qualificados, normalizar práticas operacionais e reforçar a capacitação técnica dos operadores com menor maturidade, promovendo assim um ecossistema nacional de comunicações mais resiliente e homogéneo.

3.6.4. Recomendações

A capacidade de resposta a incidentes constitui um elemento essencial para garantir a continuidade e a confiança nos serviços de telecomunicações. A análise revela fragilidades significativas nos subsectores, com destaque para a ausência de monitorização contínua, planos incompletos e baixa maturidade em práticas forenses e de coordenação interinstitucional. As recomendações abaixo visam estruturar e elevar a resposta técnica e organizacional do sector.

1. Reforço de Capacidades Internas

- Criar ou consolidar equipas especializadas em resposta a incidentes, com cobertura operacional adequada (preferencialmente 24/7).
- Garantir a actualização periódica dos planos de resposta a incidentes e a sua adequação ao perfil de risco da organização.
- Promover a adopção de soluções SIEM e sistemas IDS/IPS em todos os operadores, com foco na detecção precoce e análise eficiente de eventos.

2. Melhoria da Coordenação e Comunicação

- Fortalecer os protocolos de comunicação já estabelecidos com a Autoridade Reguladora e as entidades parceiras, garantindo uma resposta rápida e eficiente na notificação de incidentes críticos.
- Estabelecer uma Equipa de Resposta a Incidentes de Segurança nas Telecomunicações (ERIST), com o objectivo de coordenar e partilhar informações sobre ameaças de forma eficaz e em tempo real.

3. Consolidação de Planos de Contingência

- Desenvolver planos de contingência completos e testados regularmente, incluindo cenários específicos (ataques à infraestrutura, fuga de dados, falhas operacionais).
- Incluir mecanismos de preservação de evidências e análise de causa raiz, como parte do ciclo de resposta.

4. Garantia de Qualidade e Melhoria Contínua

- Implementar auditorias independentes periódicas para avaliar a eficácia dos mecanismos de resposta a incidentes.
- Estabelecer indicadores de desempenho (KPI) para monitorar a eficiência da resposta e identificar oportunidades de melhoria contínua.

5. Acompanhamento Regulatório e Diferenciação por Subsector

- Definir metas progressivas obrigatórias para os subsectores com maior défice (TV e ISP), ajustadas à sua realidade operacional.
- O Regulador deve acompanhar, de forma activa, a evolução dos níveis de maturidade, promovendo acções específicas de apoio e fiscalização.

3.7. Políticas, Processos e Procedimentos

Esta secção, composta por 9 indicadores, avaliou a existência, implementação e comunicação de políticas, processos e procedimentos relacionados com a segurança e resiliência no sector das telecomunicações.

Estes elementos são fundamentais para garantir uma postura organizacional consistente, eficaz e alinhada com os princípios de gestão de risco, assegurando que a segurança da informação e a continuidade dos serviços sejam sustentadas por práticas operacionais sólidas e integradas.

A avaliação incidiu sobre o grau de adopção formal, a aplicação prática nas operações e a comunicação interna desses mecanismos, com vista a determinar o seu real impacto na maturidade organizacional e na capacidade de resposta coordenada face a ameaças e incidentes.

3.7.1. Apreciação Geral

O sector das telecomunicações apresenta um nível de maturidade avançado (61%) na implementação de políticas, processos e procedimentos de segurança, evidenciando a existência de estruturas normativas formalizadas, embora com nível de aplicação prática ainda pouco uniforme.

Esta pontuação global reflecte a presença de directrizes bem definidas, sustentadas por normativos estruturados, mas também lacunas relevantes na operacionalização efectiva, com destaque para a falta de harmonização de procedimentos entre operadores, ausência de monitorização regular e limitações nos mecanismos de controlo interno.

A análise segmentada permite observar assimetrias significativas entre os subsectores, conforme é apresentado no gráfico abaixo.

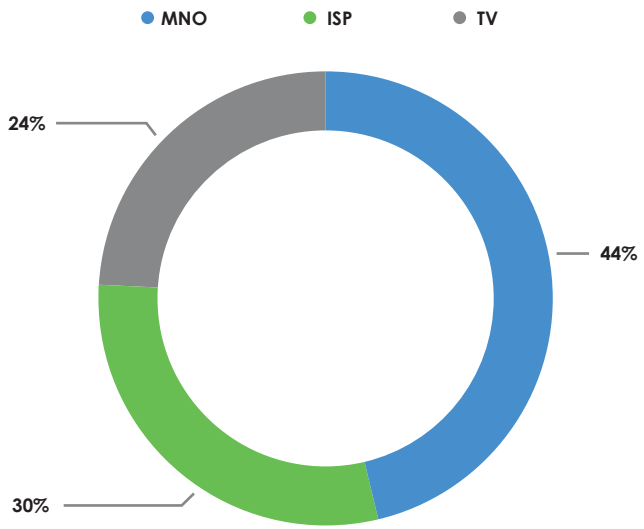


Gráfico 8: Nível de Maturidade Sectorial das Políticas e Procedimentos

A análise da dimensão relativa a políticas, processos e procedimentos revela a liderança das MNO, que alcançam (44%) da maturidade global, reflectindo uma abordagem consolidada e alinhada com padrões internacionais, políticas bem documentadas, mecanismos efectivos de implementação e verificação regular da conformidade.

As TV, com (26%), evidenciam a existência de estruturas normativas, mas enfrentam dificuldades na aplicação prática, particularmente ao nível da monitorização e do controlo operativo, o que limita a eficácia dos processos definidos.

Já os ISP, com (30%) da pontuação global, também evidenciam fragilidades. Estas prendem-se com a inexistência ou obsolescência de políticas, execução pouco rigorosa e uma comunicação interna deficiente, comprometendo a adopção uniforme das medidas de segurança e a conformidade organizacional.

3.7.2. Apreciação Detalhada por Subsector

De forma detalhada, apresentam-se as principais constatações relativas aos indicadores de Políticas, Processos e Procedimentos de segurança, com uma análise comparativa entre os três subsectores. Esta análise permite identificar os níveis de implementação das práticas essenciais para garantir continuidade de serviços, bem como as principais lacunas operacionais e estruturais que afectam a robustez das redes, segue abaixo a tabela de avaliação por subsector.

Indicadores	ISP	TV	MNO
Políticas Regulatórias	25%	13%	33%
Prazos para Incidentes	50%	25%	83%
Conformidade Legais	58%	50%	83%
Actualização de Políticas	54%	50%	83%
Objectivos Estratégico	65%	63%	100%
Monitoria de Conformidade	62%	63%	83%
Documentação de Procedimentos	58%	50%	100%
Capacitação da Equipa	65%	63%	83%
Revisão Pós-incidente	62%	50%	83%
Média	55%	47%	81%

Tabela 12: Indicadores de Políticas, Processos e Procedimentos

De forma detalhada seguem as constatações em relação à secção politica, processos e procedimentos.

1. Políticas Regulatórias

As MNO lideram (33%), evidenciando maior alinhamento das políticas internas com os requisitos regulatórios do sector. Seguem-se os ISP (25%) e as TV (13%), que apresentam dificuldades significativas na adaptação das suas políticas aos normativos aplicáveis, comprometendo a conformidade institucional.

2. Prazos para Incidentes

As MNO (83%) destacam-se pelo cumprimento de prazos, refletindo a existência de protocolos formais de notificação. Seguem-se os ISP (50%) e as TV (25%), que apresentam lacunas significativas, comprometendo a comunicação atempada com as autoridades e afetando a coordenação em situações críticas.

3. Conformidade Legais

As MNO (83%) demonstram forte adesão às exigências legais aplicáveis. Seguem-se os ISP (58%) e as TV (50%), que evidenciam dificuldades na transposição efetiva da legislação para a realidade operacional.

4. Actualização de Políticas

As MNO (83%) garantem revisões periódicas dos seus normativos, mantendo-os alinhados com as ameaças e exigências emergentes. Seguem-se os ISP (54%) e as TV (50%), que necessitam reforçar os ciclos de actualização para evitar políticas obsoletas.

5. Objectivos Estratégicos

As MNO asseguram (100%) de integração das políticas de segurança com os objectivos organizacionais, demonstrando maturidade institucional. Os ISP (65%) e a TV (63%) apresentam níveis aceitáveis, mas ainda carecem de uma articulação mais forte entre segurança e direcção estratégica.

6. Monitoria da Conformidade

As MNO, com (83%), dispõem de sistemas eficazes para garantir o cumprimento das políticas. Os ISP (62%) e as TV (63%) devem reforçar os mecanismos de supervisão interna, assegurando a aplicação prática das normas estabelecidas.

7. Documentação de Procedimentos

As MNO (100%) apresentam documentação amplamente consolidada, enquanto os ISP (58%) e as TV (50%) ainda evidenciam ausência de registos formais ou inconsistência na padronização dos procedimentos, comprometendo a eficácia das respostas operacionais.

8. Capacitação da Equipa

As MNO (83%) promovem formações regulares e direcionadas, enquanto os ISP (65%) e as TV (63%) apresentam esforços menos consistentes, indicando a necessidade de programas mais estruturados e contínuos.

9. Revisão Pós-Incidentes

As MNO (83%) mantêm bom desempenho na análise pós-incidente, permitindo a implementação de melhorias contínuas. Seguem-se os ISP (62%) e as TV (50%), que apresentam práticas ainda incipientes, com baixa formalização e limitada incorporação de lições aprendidas.

3.7.3. Conclusões

A análise da dimensão relativa a Politicas, Processos e Procedimentos confirma que, embora o sector das telecomunicações tenha atingido um nível de maturidade avançado (61%), persistem fragilidades significativas na sua aplicação prática destas medidas.

O desempenho das MNO, com (44%) da maturidade global, evidencia uma abordagem sistemática e alinhada com padrões internacionais, sustentada por documentação robusta, auditorias regulares e ciclos contínuos de actualização.

Em contraste, os ISP (30%) e as TV (26%) demonstram limitações operacionais, tanto na implementação das políticas quanto na monitorização e controlo efectivo da conformidade. Estas

diferenças apontam para a necessidade de uma maior padronização sectorial, reforço da supervisão regulatória e investimentos contínuos na capacitação técnica e na consolidação de mecanismos internos de verificação e melhoria.

3.7.4. Recomendações

A consolidação de uma cultura de segurança eficaz exige mais do que tecnologia: requer políticas claras, processos consistentes e integração transversal da segurança nas estruturas organizacionais. Esta secção apresenta recomendações orientadas ao reforço da governança, alinhamento estratégico e conformidade, com foco em padronização, desempenho e melhoria contínua.

1. Formalização e Actualização de Políticas

- As MNO devem manter a liderança como referência sectorial e partilhar modelos de políticas com os restantes operadores.
- ISP (72%) e Televisão (65%) devem criar *templates* sectoriais padrão e estabelecer ciclos obrigatórios de revisão semestrais para todas as políticas de segurança.

2. Formalização e Actualização de Políticas

- Todos os operadores devem manter políticas de segurança documentadas, aprovadas e alinhadas com as exigências regulatórias.
- Reforçar ciclos de revisão regulares (mínimo anual) e adoptar modelos sectoriais de referência para facilitar a padronização nos ISP e na TV.

3. Comunicação e Disseminação Interna

- Melhorar a comunicação interna das políticas, com acções de sensibilização recorrentes e uso de canais acessíveis.
- Garantir que todos os colaboradores conheçam as suas responsabilidades em matéria de segurança.

4. Documentação de Procedimentos

- Estabelecer guias operacionais e fluxos de trabalho documentados, assegurando consistência na aplicação das políticas.
- Verificar e assegurar que os procedimentos estejam acessíveis, actualizados e revistos em auditorias internas.

5. Capacitação e Consistência na Implementação

- Promover formação periódica obrigatória sobre políticas de segurança e conformidade.
- Criar mecanismos simples de verificação da aplicação prática (ex: listas de verificação, *checklists* de conformidade).

6. Revisão Pós-Incidentes

- Institucionalizar processos formais de revisão e lições aprendidas após incidentes.
- Assegurar que os resultados dessas análises conduzam à actualização de políticas e procedimentos.

3.8. Consciencialização e Formação

Esta secção, composta por 10 indicadores, tem como objectivo avaliar as iniciativas dos operadores e prestadores de serviços públicos de telecomunicações para educar, sensibilizar e preparar os seus colaboradores e partes interessadas em matéria de segurança da informação e protecção de dados.

A análise incidiu sobre abrangência e eficácia dos programas de formação, a percepção dos colaboradores em relação às políticas de segurança, os métodos de ensino aplicados (presenciais, digitais e simulações) e a medição do impacto real das iniciativas de consciencialização no ambiente organizacional.

3.8.1. Apreciação Geral

O sector das telecomunicações registou uma pontuação média de 52% no domínio da consciencialização e formação em segurança, o que reflecte um nível intermédio de maturidade. Embora existam iniciativas relevantes, estas ainda não cobrem sistematicamente todos os colaboradores, nem garantem a continuidade necessária para consolidar uma cultura organizacional de segurança da informação.

A análise por segmento revela disparidades expressivas, que exigem abordagens específicas para garantir equidade na capacitação dos diferentes perfis de operadores conforme demonstra o gráfico abaixo:

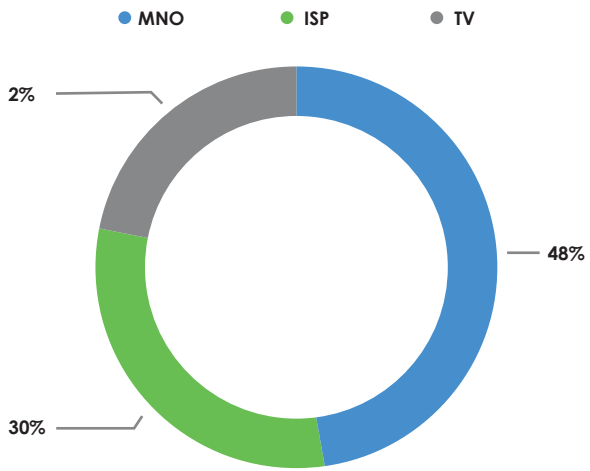


Gráfico 9: Nível de Maturidade Sectorial da Consciencialização

A análise da dimensão de Consciencialização e Formação revela um desempenho claramente liderado pelas MNO, com (74%) de maturidade global, reflectindo a implementação de programas robustos, alinhados com os riscos cibernéticos actuais. Estas operadoras destacam-se pelo uso de simulações práticas (como testes de phishing) e pela realização regular de formações obrigatórias, o que reforça uma cultura organizacional voltada para a segurança.

Em contraste, os ISP apresentam (30%) de maturidade, sustentados por estruturas formativas básicas, mas com limitações claras na abrangência dos conteúdos, na regularidade das acções e na ausência de mecanismos de avaliação.

Por sua vez, as TV, com 22%, registam o desempenho mais baixo, evidenciando graves deficiências como a inexistência de planos de formação contínua e a fraca participação dos colaboradores, o que compromete severamente a preparação do sector face a incidentes de segurança.

3.8.2. Apreciação Detalhada por Subsector

De forma detalhada, apresentam-se as principais constatações relativas aos indicadores de Conscientização e Formação, com uma análise comparativa entre os três subsectores. Esta avaliação permite identificar os níveis de implementação das práticas essenciais para garantir continuidade de serviços, bem como as principais lacunas operacionais e estruturais que impactam a robustez e a resiliência das redes, a tabela abaixo apresenta avaliação detalhado por subsector.

Indicadores	ISP	TV	MNO
Equipa Dedicada	46%	46%	67%
Políticas Actualizadas	54%	50%	83%
Plano de Resposta	58%	50%	83%
Formação	54%	50%	100%
Programas de Prevenção	31%	0%	67%
Conformidade Legal	58%	50%	83%
Recursos Financeiros	50%	25%	67%
Avaliação Periódica	54%	25%	100%
Adequação das Políticas	25%	13%	33%
Gestão de Riscos	40%	31%	58%
Média	47%	34%	74%

Tabela 13: Indicador de Consciencialização e Formação

De forma detalhada seguem as constatações identificadas na secção de conscientização e formação.

1. Equipa Dedicada

As MNO apresentam (67%) de cobertura com equipas dedicadas, assegurando uma abordagem sistematizada à capacitação. Os ISP (46%) e a TV (50%) demonstram estruturas menos robustas, com equipas muitas vezes não especializadas ou atribuídas parcialmente.

2. Políticas Actualizadas

As MNO lideram com (83%) de políticas formativas revistas de forma periódica, enquanto ISP (54%) e TV (50%) indicam práticas menos consistentes, o que pode resultar em conteúdos desactualizados face aos riscos emergentes.

3. Plano de Resposta

As MNO (83%) destacam-se na implementação de planos de resposta a incidentes, enquanto os ISP (58%) e as TV (50%) reconhecem a importância desses planos, mas ainda carecem de formalização adequada e regularidade na sua atualização.

4. Formação

As MNO lideram com (100%) na implementação de formação específica para líderes, reforçando o papel da alta direção na promoção da cultura de segurança. Em contraste, os ISP (54%) e as TV (50%) apresentam níveis médios, evidenciando a necessidade de maior envolvimento da liderança na consolidação das práticas de segurança.

5. Programas de Prevenção

As MNO lideram com (67%) na oferta de programas estruturados de prevenção, evidenciando atenção à mitigação de riscos sociais, como phishing e engenharia social. Em contraste, os ISP apresentam (31%(e as TV 0%, indicando lacunas significativas na capacitação do público externo e na promoção de práticas preventivas.

6. Conformidade Legais

As MNO lideram com (83%) de conformidade legal nos programas de formação, assegurando o alinhamento com exigências normativas e regulatórias. Em contraste, os ISP (58%) e as TV (50%) enfrentam desafios na atualização dos seus programas, comprometendo a aderência às normas legais e melhores práticas do sector.

7. Recursos Financeiros

As MNO lideram com (67%) de investimento contínuo em programas de formação, garantindo maior qualidade, frequência e abrangência das acções formativas. Em contraste, os ISP apresentam 50% e as TV 25%, evidenciando limitações financeiras que comprometem a eficácia e o alcance das iniciativas de capacitação.

8. Avaliação Periódica

As MNO lideram com (100%) na realização de avaliações periódicas dos programas de formação, permitindo ajustes baseados em evidências. Em contraste, os ISP apresentam (54%) e as TV (25%), indicando práticas ainda incipientes que comprometem a eficácia e a melhoria contínua dos programas.

9. Adequação das Políticas

As MNO destacam-se com (83%) na adequação das acções formativas aos perfis e funções dos colaboradores, garantindo maior relevância e impacto. Os ISP (58%) e as TV (50%) apresentam níveis medianos, evidenciando necessidade de alinhar conteúdos e métodos de formação às responsabilidades e riscos específicos de cada função.

10. Gestão de Riscos

As MNO lideram com (58%), evidenciando progressos na integração da formação com os planos de gestão de riscos, embora ainda exista espaço para melhoria. Em contraste, os ISP (40%) e as TV (31%) apresentam fraca articulação entre a capacitação e os planos de risco, comprometendo a eficácia das medidas preventivas.

3.8.3.Conclusão

A análise da dimensão de consciencialização e formação evidencia um nível de maturidade intermédio no sector das telecomunicações (52%), marcado por fortes assimetrias entre subsectores. As MNO destacam-se com práticas robustas, programas estruturados e alinhamento com os riscos actuais, promovendo uma cultura organizacional sólida em matéria de segurança da informação.

Em contraste, os ISP e, sobretudo, as TV apresentam fragilidades críticas, como a ausência de planos contínuos de formação, baixa participação dos colaboradores e fraca avaliação dos programas. Estas lacunas comprometem a eficácia das respostas a incidentes e a segurança do ecossistema como um todo.

Torna-se, por isso, essencial reforçar a capacitação nos segmentos menos maduros, com políticas claras, financiamento adequado e mecanismos regulares de avaliação, promovendo uma abordagem mais uniforme e coordenada a nível sectorial.

3.8.4. Recomendações

A capacitação contínua é um dos pilares para fortalecer a resiliência do sector. A análise actual evidencia assimetrias significativas entre segmentos, com o sector móvel em posição avançada e os ISP e as TV com lacunas críticas na formação de base, avaliação de impacto e alocação de recursos. As recomendações abaixo visam garantir um sistema de aprendizagem estruturado, monitorado e alinhado com os riscos emergentes.

1. Formalização de Programas e Políticas de Formação

- Todos os operadores devem estabelecer políticas formais e planos anuais de formação em segurança e protecção de dados.
- ISP e TV devem adoptar modelos-padrão sectoriais para estruturar acções formativas básicas.

2. Alocação de Recursos e Capacitação Contínua

- Garantir recursos financeiros dedicados à formação e consciencialização.
- Promover formações periódicas para todos os níveis da organização, com especial enfoque em áreas críticas e perfis executivos.

3. Integração com Gestão de Riscos e Estratégia Organizacional

- Incorporar a formação como componente transversal dos processos de gestão de riscos.
- Definir indicadores de desempenho (KPI) para medir o impacto das iniciativas de formação e consciencialização.

4. Prevenção Externa e Comunicação com Clientes

- Desenvolver campanhas educativas dirigidas aos clientes, especialmente sobre prevenção de fraudes digitais e boas práticas de cibersegurança.

5. Avaliação de Eficácia e Melhoria Contínua

- Implementar mecanismos sistemáticos de avaliação da eficácia das formações (ex: testes, simulações e *feedback*).
- Usar os resultados dessas avaliações para actualizar conteúdos e métodos de ensino com base em evidência.

6. Intervenções Prioritárias na Televisão

- Criar um plano emergencial de formação básica, com acções imediatas de capacitação interna.
- Designar responsáveis pela coordenação da segurança e formação, com metas trimestrais de cobertura e participação.

3.9. Melhoria Contínua

A secção de Melhoria Contínua é composta por nove (9) indicadores, cujo objetivo é assegurar que as organizações mantenham e reforcem, de forma sustentável, a segurança e resiliência das telecomunicações. Além da implementação de medidas técnicas e operacionais, é fundamental que estas sejam reavaliadas regularmente, garantindo eficácia, adequação e alinhamento com os objetivos estratégicos e operacionais da organização.

A análise incidiu sobre a capacidade institucional de implementar processos de revisão, atualização e aperfeiçoamento contínuo das práticas de segurança, considerando elementos como cultura organizacional orientada para a melhoria, processos de autoavaliação, envolvimento de partes interessadas, avaliação de desempenho e incorporação de lições aprendidas após incidentes.

3.9.1. Apreciação Geral

O sector das telecomunicações apresenta um nível intermédio de maturidade (52%) na implementação de processos de melhoria contínua, demonstrando uma cultura organizacional ainda pouco orientada para a revisão e optimização periódica dos mecanismos de segurança e resiliência.

Apesar deste avanço, a média global oculta disparidades significativas entre os subsectores, comprometendo a consistência da evolução e dificultando o reforço uniforme da resiliência em todo o ecossistema.

A análise desagregada permite identificar diferenças claras no grau de adopção das práticas de melhoria contínua, como demonstrado no gráfico abaixo:

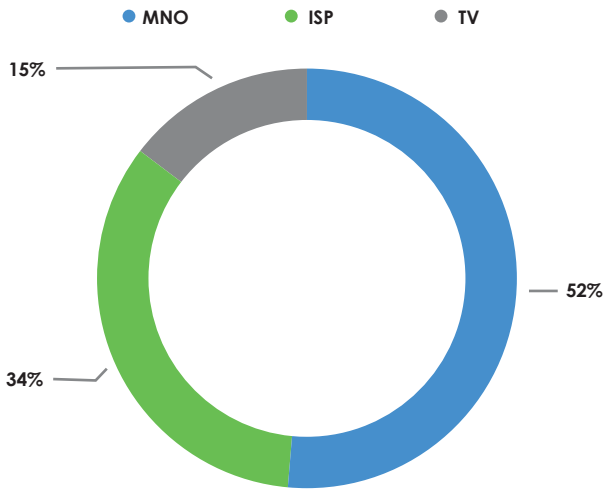


Gráfico 10: Nível de Maturidade Sectorial da Melhoria Contínua

No domínio da melhoria contínua, as MNO destacam-se com (52%) de maturidade sectorial, evidenciando uma abordagem estruturada, assente em auditorias regulares, revisões sistemáticas, integração de métricas de desempenho (KPI) e mecanismos eficazes de aprendizagem organizacional. Esta postura favorece a actualização constante face às exigências tecnológicas e regulatórias.

Os ISP, com (34%), demonstram esforços incipientes, com mecanismos básicos de auto-avaliação ainda pouco consolidados. A ausência de sistematização e fraca documentação dos processos limita a eficácia das acções correctivas e a incorporação de lições aprendidas.

Por sua vez, as TV apresentam o desempenho mais fraco, com apenas (15%), reflectindo uma ausência quase total de práticas formais de revisão, pouca participação dos intervenientes e reduzida capacidade de adaptação. Esta situação fragiliza a resiliência do subsector e a sua preparação para responder a novos desafios.

3.9.2. Apreciação detalhada por Subsector

De forma detalhada, seguem-se as principais constatações relativas aos indicadores de melhoria contínua, com uma análise comparativa entre os três subsectores. Esta análise permite identificar os níveis de implementação das práticas essenciais para garantir continuidade de serviços, bem como as principais lacunas operacionais e estruturais que afectam a robustez das redes, a tabela abaixo ilustra avaliação desta secção por subsector.

Indicadores	ISP	TV	MNO
Identificação de Melhorias	58%	35%	75%
Relatórios Anuais	45%	20%	82%
Processos de Implementação	62%	28%	88%
Monitoria da Eficácia	50%	15%	80%
Revisão de Planos	55%	25%	85%
Envolvimento de Stakeholders	40%	10%	70%
Análise de Incidentes	65%	30%	90%
Auditorias Regulares	48%	18%	78%
Alocação de Recursos	53%	22%	83%
Média	53%	23%	81%

Tabela 14: Indicadores de Melhoria Contínua

De forma detalhada seguem-se as constatações em relação a secção de melhoria continua:

1. Identificação de Melhoria

As MNO lideram com (75%), promovendo uma abordagem proactiva à detecção de oportunidades de melhoria. Os ISP apresentam (58%), evidenciando algum grau de maturidade, enquanto as TV, com (35%) mostram baixa sistematização nesse processo, limitando o avanço da segurança e da resiliência organizacional.

2. Relatórios Anuais

As MNO lideram com (82%), garantindo produção consistente de relatórios anuais que suportam a análise histórica e a definição de planos de acção baseados em evidências. Os ISP registam (45%), mostrando documentação ainda insuficiente, enquanto as TV, com (20%), apresentam cobertura muito limitada, comprometendo o acompanhamento e melhoria contínua das práticas de segurança.

3. Processos de Implementação

As MNO lideram com (88%) de concretização de melhorias, evidenciando forte capacidade de execução e incorporação eficaz de ações correctivas. Seguem os ISP, com (62%), demons-

trando progresso, mas ainda com margem para reforço da eficácia operacional. Já as TV, com (28%), apresentam fragilidades significativas na implementação prática, limitando a efetividade das ações de melhoria contínua.

4. Monitoria da Eficácia

As MNO lideram com (80%), realizando medição sistemática dos resultados e garantindo acompanhamento contínuo da eficácia das melhorias implementadas. Os ISP apresentam (50%), demonstrando práticas de monitoria limitadas, enquanto as TV, com apenas (15%), não avaliam de forma consistente o impacto das melhorias, comprometendo a correção de falhas e o reforço das práticas eficazes.

5. Revisão de Planos

As MNO lideram com (85%), garantindo revisões periódicas e sistemáticas dos planos de segurança. Os ISP apresentam (55%), indicando práticas de revisão ainda insuficientes, enquanto as TV, com apenas (25%), carecem de processos regulares de atualização, ficando vulneráveis a planos desatualizados e pouco eficazes.

6. Envolvimento de *Stakeholders*

As MNO lideram com (70%), evidenciando boa articulação com áreas internas e externas no processo de melhoria contínua. Os ISP apresentam (40%), mostrando envolvimento limitado, enquanto as TV, com apenas (10%), mantêm uma abordagem compartimentada, dificultando a visão sistémica dos riscos e das acções necessárias.

7. Análise de Incidentes

As MNO lideram com (90%), demonstrando utilização eficiente das lições aprendidas após incidentes. Os ISP apresentam (65%), incorporando parcialmente este processo, enquanto as TV, com apenas (30%), ainda não sistematizam a análise pós-incidente, perdendo uma fonte crítica de melhoria contínua.

8. Auditorias Regulares

As MNO lideram com (78%), realizando verificações periódicas e consistentes. Os ISP apresentam (48%), com auditorias menos frequentes, e as TV registam apenas (18%), evidenciando deficiências na detecção de falhas e na responsabilização interna.

9. Alocação de Recursos

As MNO lideram com (83%) de financiamento adequado, assegurando capacidade de implementação das melhorias. Os ISP apresentam (53%), enquanto as TV registam apenas (22%), evidenciando que a escassez de recursos limita significativamente o progresso dos subsectores menos maduros.

3.9.3. Conclusão

A análise da dimensão de Melhoria Contínua revela que, embora o sector das telecomunicações em Moçambique apresente uma maturidade intermédia (52%), persistem disparidades acentuadas entre os subsectores, comprometendo a evolução integrada da segurança e resiliência no ecossistema.

As MNO destacam-se com práticas consolidadas, demonstrando forte cultura organizacional voltada para a revisão sistemática, aprendizagem operacional e uso eficaz de métricas e auditorias. Esta abordagem traduz-se numa capacidade elevada de adaptação às exigências tecnológicas e regulamentares.

Por outro lado, os ISP ainda operam com estruturas básicas e pouco formalizadas, limitando a eficácia das melhorias implementadas. Quanto aos segmentos das TV, revelam uma situação crítica, com ausência de processos estruturados, fraca articulação interna e investimento reduzido, o que fragiliza a capacidade de resposta e evolução contínua. Estes resultados sublinham a necessidade de reforçar os mecanismos de governação e financiamento, particularmente nos subsectores menos desenvolvidos, a fim de garantir uma progressão mais homogénea e sustentável em todo o sector.

3.9.4. Recomendação

A adopção de uma cultura de melhoria contínua é essencial para a maturação organizacional e a sustentabilidade dos processos de segurança, qualidade e inovação. O sector apresenta níveis díspares de avanço, sendo necessário reforçar práticas estruturadas, integrar metodologias de gestão da qualidade e investir em capacitação específica. As recomendações a seguir promovem um ciclo permanente de evolução organizacional.

1. Formalização e Padronização de Processos

- Todos os operadores devem estabelecer procedimentos formais para a identificação, implementação e monitorização de melhorias.
- Criar guias sectoriais com boas práticas e formatos de relatório padronizados, a serem partilhados com todos os subsectores.

2. Avaliação e Monitoria Contínua

- Implementar ciclos regulares de revisão de planos de segurança (mínimo anual), com evidência documental.
- Adoptar métricas e indicadores de desempenho (KPI) para avaliar a eficácia das melhorias implementadas.

3. Integração da Análise de Incidentes

Garantir que todos os incidentes de segurança sejam revistos formalmente, com produção de relatórios de lições aprendidas e actualização de procedimentos.

4. Reforço das Auditorias Internas e Externas

Promover a realização de auditorias técnicas e de conformidade de forma periódica, especialmente entre ISP e TV, com foco na avaliação da melhoria contínua.

5. Envolvimento de Partes Interessadas

Incentivar a participação de diferentes áreas da organização na revisão de planos e processos, garantindo uma visão transversal e mais eficaz da segurança.

6. Alocação Sustentada de Recursos

- Assegurar financiamento regular e dedicado à implementação de melhorias identificadas em auditorias, relatórios e revisões internas.
- O Regulador pode avaliar incentivos a operadores que demonstrem progressos efectivos em maturidade de melhoria contínua.

7. Intervenções Específicas por Subsector

- As MNO devem manter os níveis actuais, partilhar boas práticas e apoiar tecnicamente os demais segmentos.
- Os ISP devem reforçar a consistência e a periodicidade dos processos, com apoio metodológico.
- As TV devem implementar um plano mínimo de melhoria contínua, com suporte externo e metas trimestrais de evolução.

4

CONSIDERAÇÕES FINAIS

4. Considerações Finais

O presente relatório apresenta uma avaliação abrangente sobre o nível de maturidade em segurança e resiliência do sector das telecomunicações em Moçambique. A análise baseou-se num conjunto representativo de 22 operadores que responderam integralmente ao questionário enviado, subdivididos em três subsectores, cuja amostra é descrita abaixo

- Telefonia Móvel (MNO): 3 operadores;
- Serviço de Televisão (TV): 4 operadores; e
- Provedores de Internet (ISP): 15 operadores.

O estudo permitiu identificar os pontos fortes, lacunas operacionais e estruturais, bem como as assimetrias existentes entre os subsectores, oferecendo uma visão consolidada sobre o estado atual da segurança da informação, preparação para incidentes, políticas, formação e melhoria contínua no sector.

Os resultados evidenciam que as MNO lideram em praticamente todos os domínios analisados, demonstrando maturidade elevada, práticas consolidadas e cultura organizacional orientada à resiliência. Por outro lado, os ISP e, sobretudo, as TV apresentam fragilidades significativas, com impactos na implementação prática das políticas, comunicação interna, resposta a incidentes e capacitação de equipas.

4.1. Principais Constatações

A análise comparativa dos resultados por dimensão temática permite evidenciar padrões consistentes de desempenho entre os subsectores. As diferenças de maturidade observadas não são meramente pontuais, mas reflexo de assimetrias estruturais e operacionais que impactam directamente na segurança e a resiliência do sector. Os pontos abaixo destacam os principais contrastes e fragilidades comuns identificados no exercício de avaliação.

1. Desempenho Assimétrico entre Subsectores

- As MNO evidenciam nível de maturidade elevado (80%), sendo líderes em controlos de segurança com (98%), resposta a incidentes com (85%) e melhoria contínua com 81%, posicionando-se como referência no sector.
- Os ISP com (48%) e as TV com (43%) apresentam desempenhos substancialmente inferiores, com carências evidentes em formação, documentação, partilha de informação e gestão de incidentes.

2. Fragilidades Sistémicas Identificadas

- A cooperação entre operadores é limitada, com uma pontuação média de (35%), afectada principalmente pela fraca articulação dos ISP (21%) e das TV (11%) com o regula-

dor e entre si.

- A gestão de fraudes com um nível de maturidade de 39%, a disparidade é notável, sendo que, enquanto as MNO implementam sistemas sofisticados representando uma posição de (73%), os ISP com (20%) e as TV com (25%) operam com mecanismos rudimentares ou inexistentes.
- A protecção de dados com (61%) global, tem registado progressos, mas a conformidade regulatória continua aquém do exigido nos segmentos mais frágeis.
- Em termos de resiliência de rede com uma percentagem de nível de maturidade de (63%), destaca-se a robustez da MNO com (75%), face à vulnerabilidade crítica dos ISP com (53%), em áreas como redundância, continuidade e comunicação de incidentes.
- A formação e consciencialização representando o nível de maturidade de (52%), permanece desigual, e as MNO com (74%) dispõem de programas estruturados, enquanto os ISP com (47%) e as TV com (34%), mostram baixos níveis de investimento e cobertura.

4.2. Oportunidades de Melhoria

Com base nos resultados da avaliação, foi possível identificar cinco (5) áreas estratégicas prioritárias que, se adequadamente exploradas, poderão acelerar o processo de amadurecimento do sector das telecomunicações em Moçambique. Estas oportunidades visam colmatar as fragilidades detectadas, promover a harmonização das práticas entre subsectores e consolidar uma abordagem integrada à segurança e resiliência. Destacam-se, a seguir, os principais eixos de actuação recomendados:

- Padronização e disseminação de boas práticas, especialmente nos segmentos menos maduros.
- Fortalecimento dos mecanismos de cooperação e partilha de informação com o regulador.
- Capacitação técnica contínua, com enfoque em formação prática e simulações de ciberincidentes.
- Investimento em tecnologia avançada, incluindo automação, inteligência artificial e detecção proactiva de ameaças.
- Criação de mecanismos formais de auditoria, responsabilização e avaliação de desempenho.

4.3. Recomendações Estratégicas

A consolidação de um sector das telecomunicações seguro, resiliente e alinhado com os padrões internacionais requer uma actuação estratégica multissectorial, que vá para além da correcção pontual de fragilidades. Com base nos resultados da avaliação e nas lacunas identificadas ao longo das nove dimensões analisadas, propõem-se 11 (onze) recomendações

prioritárias, adaptadas à realidade nacional, mas fortemente inspiradas em boas práticas internacionais de cibersegurança, gestão de risco e resiliência organizacional.

Estas recomendações têm como objectivo orientar os operadores, o regulador e os restantes actores do ecossistema na definição de políticas públicas, investimentos e reformas estruturais que impulsionem a maturidade cibernética em todo o sector:

1. Regulamentação e Supervisão Activa

- Definir requisitos mínimos obrigatórios por segmento, com metas graduais e ajustadas ao perfil de risco.
- Reforçar a fiscalização periódica, acompanhada de mecanismos de incentivo ao cumprimento.

2. Fortalecimento da Cooperação

- Criar plataformas sectoriais para partilha de ameaças, indicadores e boas práticas.
- Promover exercícios conjuntos de resposta a incidentes, integrando operadores e entidades públicas.

3. Investimento em Tecnologia e Capacitação

- Adoptar soluções automatizadas de segurança (ex.: SIEM, DLP, criptografia).
- Desenvolver programas de formação contínua, com simulações realistas (*phishing, ransomware* e falhas técnicas).

4. Resiliência Operacional

- Assegurar redundância de sistemas críticos, planos testados e *backups*.
- Estabelecimento de mecanismos de segurança e resiliência das redes e centros de dados.
- Estabelecer redes redundantes por via de partilha de infra-estrutura por forma a garantir alta disponibilidade das redes.
- Reforçar a comunicação com os clientes em situações de crise, garantindo transparência e confiança.

5. Melhoria Contínua

- Institucionalizar processos de avaliação pós-incidente e auditorias regulares.
- Definir indicadores de desempenho (KPI) para medir a evolução da maturidade cibernética.

6. Governança e Responsabilização

- Estabelecer métricas de *accountability*, incluindo penalizações por incumprimentos operacionais.
- Publicar um relatório anual de maturidade por operador, promovendo transparência e *benchmarking*.

7. Segurança da Cadeia de Fornecimento

- Avaliar fornecedores críticos (ex.: cloud, datacenters) e exigir conformidade contratual com normas sectoriais.
- Implementar requisitos mínimos de segurança para terceiros.

8. Gestão de Crises e Comunicação Pública

- Desenvolver um plano sectorial de comunicação em crises cibernéticas.
- Realizar exercícios públicos de simulação, envolvendo operadores, regulador e utilizadores estratégicos.

9. Apoio a Pequenos Operadores

- Criar fundos sectoriais e programas de assistência técnica para ISP de pequena escala.
- Promover modelos de segurança partilhada e centros de competência intersectoriais.

10. Protecção de Infraestruturas Críticas

- Mapear, classificar e proteger as infra-estruturas críticas nacionais (ex.: cabos submarinos, nós de rede, *data centers*).
- Imposição de requisitos técnicos e operacionais reforçados.

11. Envolvimento da Sociedade

- Lançar campanhas públicas de sensibilização sobre fraudes digitais (ex.: SIM *swap, phishing*, entre outras).
- Criar um selo de confiança para operadores que cumpram normas avançadas de segurança.

4.4. Conclusão

O presente Relatório sobre o Nível de Maturidade da Segurança e Resiliência das Telecomunicações em Moçambique evidencia, de forma clara e objectiva, os avanços alcançados e

os desafios ainda persistentes no sector. A avaliação abrangente realizada a vinte e duas (22) entidades permitiu identificar padrões, disparidades e tendências estruturais críticas que afectam a capacidade de resposta, a continuidade dos serviços e a confiança no ecossistema nacional de comunicações.

Constatou-se que as MNO assumem uma posição de liderança, apresentando níveis de maturidade avançados em quase todas as dimensões analisadas, nomeadamente no controlo de segurança, gestão de incidentes, protecção de dados e melhoria contínua. Tal desempenho reflecte o investimento contínuo, a adopção de boas práticas internacionais e uma postura proactiva face às ameaças emergentes.

Em contraste, os ISP e as TV registam níveis de maturidade substancialmente inferiores, com fragilidades evidentes em domínios essenciais como a cooperação sectorial, gestão de fraudes, consciencialização interna e formalização de políticas de segurança. Estas debilidades comprometem a resiliência global do sector e revelam a necessidade urgente de intervenções estratégicas específicas e diferenciadas.

A análise sectorial revelou ainda fragilidades sistémicas, particularmente na articulação institucional, na padronização de práticas, no reforço da protecção de dados e no alinhamento efectivo com os referenciais normativos e legais. A ausência de processos estruturados de melhoria contínua e de mecanismos eficazes de partilha de informação aumenta o risco de vulnerabilidades críticas, num contexto em que as ameaças cibernéticas se tornam cada vez mais sofisticadas e imprevisíveis.

Neste sentido, a implementação das recomendações estratégicas propostas neste relatório que incluem a definição de requisitos normativos claros, o reforço da supervisão regulatória, o investimento em tecnologias de detecção e resposta, a capacitação contínua dos recursos humanos e a criação de plataformas colaborativas sectoriais, é imperativa para garantir uma evolução sustentada e harmonizada do sector.

O sucesso da transformação digital em Moçambique estará intrinsecamente ligado à capacidade do sector das telecomunicações de consolidar uma postura robusta de segurança e resiliência. Tal consolidação exige o compromisso inequívoco de todos os actores, operadores, regulador e Estado, numa visão conjunta e coordenada de desenvolvimento sustentável, inovação segura e protecção eficaz dos interesses dos cidadãos e das infra-estruturas críticas nacionais.

A construção de um sector seguro, resiliente, confiável e competitivo não é apenas uma necessidade estratégica; é uma condição sine qua non para garantir a estabilidade económica, a confiança social e o pleno aproveitamento das oportunidades da era digital. Este relatório constitui, assim, não apenas um diagnóstico detalhado, mas também uma ferramenta estratégica de orientação para a acção colectiva e para a modernização efectiva das telecomunicações em Moçambique.

4.5.Detalhes da Elaboração do Relatório

	Fase	Actividades Principais	Responsáveis	Resultados Esperados
1	Planeamento Inicial	Definição dos objectivos, âmbito, metodologia e cronograma	UCTT	Termos de referência do estudo e plano de actividades
2	Desenho Metodológico	Construção do questionário técnico e validação	UCTT	Instrumento de recolha de dados validado
3	Recolha de Dados	Envio dos inquéritos, recepção e verificação da informação	UCTT/ Operadores	Dados recolhidos junto dos operadores e entidades do sector
4	Análise e Tratamento dos Dados	Sistematização, codificação, estatísticas descritivas e análise por indicadores	UCTT	Tabelas, gráficos e matrizes analíticas
5	Redacção do Relatório	Redacção técnica das secções temáticas e consolidação da informação analisada	UCTT	Versão preliminar do relatório
6	Revisão e Validação Interna	Revisão técnica, incorporação de comentários, verificação de consistência e coerência	UCTT/ Entidade contratada	Versão final validada internamente
7	Submissão e Aprovação Institucional	Apresentação ao CA, revisão final e despacho de aprovação	Conselho de Administração – INCM	Relatório aprovado e pronto para divulgação
8	Divulgação e Partilha	Envio do relatório às partes interessadas, publicação em meios institucionais	UCTT / Gabinete de Comunicação	Relatório disponibilizado ao público e entidades parceiras

INCM

Autoridade Reguladora das Comunicações