BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

12.º SUPLEMENTO

IMPRENSA NACIONAL DE MOÇAMBIQUE, E. P.

SUMÁRIO

CONSELHO DE MINISTROS

Resolução n.º 69/2021

de 31 de Dezembro

Havendo necessidade de aprovar a Política de Segurança Cibernética e Estratégia de sua implementação, com vista a adequá-la aos instrumentos orientadores e aos desafios impostos pelo crescente progresso das Tecnologias de Informação e Comunicação (TICs), tendo nas acções estratégicas de segurança cibernética o alicerce para combater o crime cibernético, no uso das competências que lhe são atribuídas pela alínea *f*) do n.º 1 do artigo 203 da Constituição da República, o Conselho de Ministros determina:

Artigo 1. É aprovada a Política de Segurança Cibernética e Estratégia da sua Implementação, em anexo, que é parte integrante da presente Resolução.

Art. 2. A presente Resolução entra em vigor na data da sua publicação.

Aprovada pelo Conselho de Ministros, aos 31 de Agosto de 2021.

Publique-se.

O Primeiro-Ministro, *Carlos Agostinho do Rosário*.

Política de Segurança Cibernética e Estratégia da sua Implementação

1. Introdução

A era digital coloca países de todo o mundo perante um novo conceito de segurança, o de segurança cibernética, que deve ser encarado com responsabilidade e envolvimento de todas as forças vivas da sociedade, para que Moçambique possa tirar o melhor proveito do espaço cibernético.

Para efeitos do presente documento entende-se por espaço cibernético ao ambiente complexo, de valores e interesses, materializado numa área de responsabilidade colectiva, que resulta da interacção entre pessoas, redes e sistemas de informação, e por segurança cibernética ao conjunto de medidas e acções de prevenção, monitorização, detecção, reacção, análise e correcção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no espaço cibernético, e das pessoas que nele interagem. A segurança cibernética inclui todas as medidas legais, tecnológicas e processos que visam proteger pessoas, colectivas e singulares, e bens, com destaque para as infra-estruturas críticas de informação, no espaço cibernético.

A PENSC vai ao encontro dos anseios dos moçambicanos no sentido de criarem uma visão nacional que lhes permita desenvolverem uma plataforma comum de resiliência a ataques cibernéticos ou a quaisquer outras formas de perturbação da ordem pública, com recurso às Tecnologias de Informação e Comunicação (TIC).

As preocupações com a segurança cibernética vêm se avolumando desde que o país decidiu enveredar pela massificação do uso das TIC, quando o Governo aprovou a primeira Política de Informática, através da Resolução n.º 28/2000, de 12 de Dezembro, que 18 anos depois foi revista e aprovada sob a nova perspectiva de Política para a Sociedade da Informação, através da Resolução n.º 17/2018, de 21 de Junho.

A PENSC é um instrumento parte da materialização da Política para a Sociedade de Informação que vai orientar os esforços de Moçambique na resolução dos novos problemas trazidos pela revolução tecnológica, que passa por acções que garantam:

1. A regulamentação de funcionamento do espaço cibernético;
2. O desenvolvimento de capacidade institucional e operacional em matéria de segurança cibernética;

3. A protecção de infra-estruturas críticas e activos de informação;
4. O ordenamento da coordenação e colaboração institucional em matéria de segurança cibernética;
5. A promoção de boas práticas no uso das TIC.

A PENSC complementa uma série de outros instrumentos orientadores e regulatórios do sector das TIC que foram sendo aprovados e implementados pelo Governo ao longo dos últimos anos, dos quais se destacam a Política para a Sociedade da Informação, a Lei de Transacções Electrónicas, Lei n.º 3/2017, de 9 de Janeiro, a Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho, o Regulamento do Quadro de Interoperabilidade de Governo Electrónico, o Decreto n.º 67/2017, de 1 de Dezembro, o Regulamento de Segurança de Redes de Telecomunicações, Decreto n.º 62/2019, de 1 de Agosto, o Regulamento do Sistema de Certificação Digital de Moçambique, Decreto n.º 59/2019, de 1 de Dezembro, o Regulamento do Domínio ".mz", Decreto n.º 82/2020, de 10 de Setembro, a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, Resolução n.º 5/2019, de 20 de Junho e as recentes iniciativas legislativas no que se refere ao Código Penal, que, de um modo geral, permitiram dar cobertura universal aos crimes de natureza informática no país.

A 14.ª sessão ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana, sobre as TIC em África realizada sob o lema Desafios e Perspectivas para o Desenvolvimento, orientou cada Estado membro a elaborar uma Política Nacional de Segurança Cibernética que reconheça a importância da Infra-estrutura da Informação Crítica (IIC), identificar os riscos que enfrenta e definir a forma de alcançar os objectivos dessa política.

O Trabalho da preparação da presente Política e Estratégia Nacional de Segurança Cibernética (PENSC) enquadra-se não só nas orientações emanadas na 14.ª sessão ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana, sobre as TIC, mas também no cumprimento do artigo 24 da Resolução n.º 5/2019, de 20 de Junho, Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, que recomenda os Estados membro a estabelecerem um quadro regulamentar composto pela política e estratégia nacional de segurança cibernética que visam definir, coordenar e implementar iniciativas e prioridades relativas a protecção das instituições, pessoas e bens contra incidentes decorrentes do uso das TIC no espaço cibernético.

Todas as iniciativas que constam da PENSC concorrem para a melhoria da avaliação do país nos indicadores internacionais de segurança cibernética, bem como para a promoção de uma imagem de um país seguro e atractivo ao investimento.

A PENSC é um instrumento chave que o país precisa para melhor definir e coordenar as iniciativas e prioridades no âmbito da utilização segura das TIC, a fim de proteger instituições públicas e privadas, pessoas e bens contra-ataques cibernéticos, em alinhamento com as convecções regionais e internacionais.

Nos capítulos que se seguem, é feita a contextualização da PENSC, seguida da apresentação da Visão, Missão, Objectivos, Princípios Orientadores, Pilares, Factores Críticos de Sucesso e da sua Estratégia de Implementação.

2. Política Nacional de Segurança Cibernética

Moçambique, a exemplos de muitos países, tem vindo a adoptar leis, políticas e estratégias que promovem o uso e o desenvolvimento de Tecnologias de Informação e Comunicação (TIC) por reconhecer que estas, têm um papel importante como catalisadoras dos processos de modernização e transformação digital, pois servem de plataformas de suporte em várias áreas de desenvolvimento económico e social como a agricultura, educação, saúde, energia, turismo, exploração de recursos naturais, economia e finanças, de entre outras.

O espaço cibernético promove mercados abertos e sociedades abertas catapultando o desenvolvimento das nações. Porém, essa mesma abertura também pode tornar os internautas mais vulneráveis a criminosos, serviços de contrainteligência de entidades estrangeiras e outros tipos de ataques cibernéticos com vista a prejudicar, comprometer ou danificar as infra-estruturas críticas e activos de informação no geral e a integridade do cidadão e do Estado em particular.

A presente Política Nacional de Segurança Cibernética e a sua Estratégia de Implementação (PENSC) visam mitigar os efeitos dos ataques e incidentes cibernéticos no nosso país.

a. Dados de base

Multiplicam-se no país nos últimos anos o assédio e abuso no espaço cibernético, a propagação de informação falsa, as burlas, o roubo de identidade, crimes financeiros, o ciberterrorismo e outros crimes informáticos. Estes actos afectam a vida económica e social, para preocupação das autoridades que têm que lidar com matérias de garantia da segurança e da soberania nacional e que devem tralhar no sentido de garantir um espaço digital credível para a protecção das infra-estruturas críticas de informação, da privacidade e das liberdades do cidadão e para o combate ao crime cibernético.

i. Situação do país no contexto da segurança cibernética

O referencial geográfico do espaço cibernético de Moçambique compreende uma área de 801.537 quilómetros quadrados do território nacional e os seus 2.770 quilómetros da costa marítima, onde vivem actualmente cerca de 30 milhões de habitantes, segundo as projecções do último censo populacional, realizado em 2017. Cerca de 66% desta população está concentrada nas zonas rurais, dominadas por solos aráveis, bacias hidrográficas, recursos minerais e energéticos, em quantidades consideráveis.

Moçambique, país detentor de enormes reservas de gás natural na sua plataforma marítima continental, pode vir a tornar-se, a médio prazo, num dos maiores exportadores de hidrocarbonetos, capitalizando os ganhos na recuperação e desenvolvimento socioeconómico, em benefício das suas populações.

Os esforços de recuperação e desenvolvimento nacional tem sido contrariado, porém, pelos efeitos negativos das mudanças climáticas, que, ciclicamente, vem afectando de forma negativa o crescimento do Produto Interno Bruto (PIB) do país, que em 2019 se fixou abaixo da média (3.7%) registada entre 2016 e 2018, o mais baixo crescimento desde as cheias devastadoras de 2000.

O Relatório da União Internacional de Telecomunicações (UIT) sobre o Índice Global de Segurança Cibernética (GCI) de 2018 colocou Moçambique entre os países com o pior nível de Segurança Cibernética, com base na análise das seguintes categorias: i) Medidas legais; *ii*) medidas técnicas; *iii*) medidas organizacionais; *iv*) desenvolvimento de capacidades; e *v*) cooperação internacional. Por isso, num *ranking* de 194 países, Moçambique ocupou as posições 26 e 132, no índice continental e global respectivamente.

No Relatório do Índice Global de Segurança Cibernética de 2020 divulgado pela União Internacional de Telecomunicações (UIT), agência do sector de tecnologias da ONU, Moçambique subiu 9 posições, tendo passado da posição 132 em 2018 para a posição 123 numa lista com 193 países avaliados. O Índice Global de Segurança Cibernética da UIT avalia as acções que os países empreendem com o objectivo de fomentar a consciencialização sobre os compromissos das nações em relação a segurança

cibernética e identificar os pontos fortes e as áreas onde são necessárias melhorias, além de partilhar as boas práticas de segurança cibernética.

A posição conquistada pelo nosso país nos dois últimos relatórios da UIT do Índice Global de Segurança Cibernética demostra o compromisso crescente de Moçambique e do Governo com a segurança cibernética a nível nacional, regional, continental e global, e em particular com o aumento da consciência da sociedade sobre a importância das diferentes dimensões de segurança cibernética e o nível de envolvimento de país no desenvolvimento e na segurança do espaço cibernético.

Um importante indicador socioeconómico normalmente usado para avaliar os países é o Índice do Desenvolvimento Humano (IDH). Em 2020 Moçambique reduziu uma posição, tendo passado da posição 180º para 181º numa lista com 189 Estados-membros das Nações Unidas avaliados, do total dos 193 Membros das Nações Unidas.

O outro instrumento importante é o indicador de negócios, o *Doing Business*. Moçambique continua com índices de desempenho baixos no *Doing Business*, pois no *ranking* global de 2020, que avaliou 189 países, o país reduziu três posições, tendo passado da posição 135º em 2019 para a posição 138º em 2020. O Relatório do *Doing Business de 2000*, uma das principais publicações do Banco Mundial, é a 17ª edição de um estudo anual que avalia como as leis e instrumentos legais promovem ou restringem as actividades empresariais.

A Decisão do Conselho Executivo da União Africana EX.CL/Dec. 1074 que aprovou a Estratégia de Transformação Digital para África solicitou à Comissão da União Africana para desenvolver a sua matriz de implementação que preconize o desenvolvimento de uma sociedade digital e económica inclusiva em África. A presente estratégia está alinhada com as cinco áreas transversais da Estratégia de Transformação digital para África (2020-2030), concretamente no que concerne ao tema de segurança cibernética e protecção de dados pessoais.

A PENSC é um importante instrumento orientador da governação, não só porque foi preparada para atender aos anseios dos moçambicanos no domínio de segurança cibernética, mas porque concorre para que o país se conforme com uma das grandes preocupações de actualidade em todo o mundo no âmbito do desenvolvimento da Sociedade Global da Informação.

ii. Uso das TIC

A crescente digitalização de serviços no nosso país tem resultado em profundas transformações económicas, sociais e culturais, bem como em substanciais melhorias de governação e da vida das populações.

Para avaliar o nível de desenvolvimento e utilização das TIC entre países é usado o estudo comparativo designado Índice de Desenvolvimento das TIC (IDI - ICT *Development Index*), que mostra a situação de cada país nos diferentes aspectos de uso das TIC nas áreas prioritárias de desenvolvimento social e económico como a educação, a saúde, a agricultura, energia, turismo, dentre outras.

No último Relatório do Índice de Desenvolvimento das TIC (IDI - *ICT Development Index*) publicado em 2017 Moçambique ficou na posição 150, tendo reduzido três posições relativamente a 2016, num *ranking* de 176 países, apesar dos esforços que o Governo tem feito para investir em infra-estruturas, promoção do acesso e disseminação do uso de TIC.

A face mais visível do impacto da digitalização da economia nacional, para maioria da população, sobretudo nas zonas rurais e outras classes menos favorecidas, são os serviços de dinheiro móvel, nomeadamente as plataformas Mkesh, Mpesa e e-Mola, entre outras formas de transacção electrónica a nível dos produtos e serviços financeiros básicos como o pagamento de água e de electricidade.

O Governo de Moçambique, consciente desta situação, desenvolveu a Estratégia Nacional de Inclusão Financeira (2016-2022), que se enquadra na Estratégia do Desenvolvimento do Sector Financeiro. Um dos enfoques chave desta estratégia está no aumento da acessibilidade a serviços financeiros pela população, especialmente nas áreas rurais. O serviço de dinheiro móvel é um dos canais que está a ser mais usado para se acelerar a inclusão financeira oferecendo uma alternativa aos serviços financeiros formais. Com os serviços de dinheiro móvel mais moçambicanos anteriormente excluídos do ponto de vista financeiro obtiveram acesso a serviços através de plataformas digitais de serviços de dinheiro móvel.

No que toca a inclusão digital, importa realçar a expansão das praças digitais, que permitem o acesso grátis à *Internet*. Como resultado, até meados de 2020, tinham sido instaladas ao todo 69 praças digitais em diferentes regiões do país.

O serviço de telefonia móvel atingiu em 2019 14,908,191 assinantes, uma cobertura que aproxima o país das tendências regionais e mundiais, em termos de acesso à telefonia. O indicador inclui o número de assinantes pós-pagos e o número de assinantes pré-pagos activos e aplica-se a todos os assinantes de telefonia móvel que oferecem comunicações de voz. Exclui assinantes via cartões de dados ou modems USB e assinantes de serviços públicos de dados móveis.

O número de assinantes de *Internet* em 2019, isto é, assinantes activos da banda larga móvel, foi de 5,505,202. Este refere-se ao somatório dos assinantes activos da banda larga móvel usando o telefone celular e o computador (porta USB) para o cidadão ter acesso à *Internet*.

Ainda na área das telecomunicações, são de destacar outros grandes progressos alcançados pela indústria da comunicação, nomeadamente as tecnologias Long Term Evolution (LTE) e *Internet* das Coisas (IoT), que estão na dianteira da digitalização.

A nível da Administração Pública, foram implementados projectos e iniciativas de TIC, com impacto social e governativo, sendo de destacar:

1. Rede Electrónica do Governo (GovNet), em 2020 interligava 11 províncias e 139 distritos dos 154 distritos do país;
2. Sistema de Administração Financeira do Estado (e-SISTAFE);
3. Sistema de Registo e Facilitação Empresarial (eBAU);
4. Sistema de Registo e Identificação do Cidadão;
5. Sistema de Gestão da Terra e da Propriedade;
6. Janela única Electrónica;
7. Sistema de pagamento de Impostos (e-Tributação);
8. Sistema de controlo fronteiriço e Migratório;
9. Sistema de Gestão de Beneficiários de Segurança Social;
10. Sistema de Gestão de Recursos Humanos do Estado.

A nível da educação, no ensino superior e no ensino técnico em particular, há a registar o estabelecimento da Rede de Instituições de Ensino Superior e de Investigação de Moçambique, a MoRENet (*Mozambique Research and Education Network*), que em finais de 2020 interligava 180 instituições de ensino superior, de ensino técnico profissional e de investigação distribuídas por todas as províncias do país disponibilizados serviços digitais aos membros das comunidades académica científicas assentes nas diversas aplicações de plataformas digitais de apoio aos processos de ensino e aprendizagem e de gestão académica e pedagógica.

Houve progressos também no processo de migração digital, que permite a televisão passar a transmitir em ambiente de

convergência, possibilitando-lhe conectar-se com qualquer outra plataforma digital, nomeadamente computadores e celulares, conferindo-lhe maior interactividade e capacidade de programação. Tudo indica que, até ao fim de 2021, todos os estúdios de rádio-televisão vão passar a operar em ambiente digital, sendo a rede de distribuição coberta em 90%.

iii. Ameaças cibernéticas

À medida que o uso das TIC aumenta, cresce também a exposição do país a ataques e outro tipo de incidentes cibernéticos, entre crimes contra infra-estruturas críticas, sistemas, pessoas, espionagem política e empresarial, ciberguerra entre outros. É o caso das páginas de *Internet*, que têm sido alvo preferencial das acções criminosas, tanto na forma tentada como consumada. Outro alvo preferencial é o sector financeiro, sobretudo o bancário, através de clonagem de cartões, *phishing*, roubo de identidade, entre outras formas de ataques cibernéticos. Crescem também de forma exponencial, os ataques de sequestro de identidade (*ransomware*), bem como os ataques cibernéticos perpetrados na "*Dark web*" e "*deep web*", no qual funciona uma espécie de mercado livre mundial do crime que proporciona actividades tais como tráfego de droga, terrorismo (actores estatais e não estatais), sabotagem, tráfego de pessoas, lavagem de dinheiro, venda de armas, contratação de assassinos ou outros tipos de criminosos, comércio de órgãos humanos, pornografia infantil, venda de listas com números e códigos de cartões de crédito válidos, de entre outras actividades ilícitas. As transacções económicas e financeiras neste espaço são realizadas através de criptomoeadas digitais, procurando assim garantir o anonimato completo do negócio. Os ataques cibernéticos perpetrados a partir de dispositivos móveis também aumentam e facilitam de certa forma a operação dos internautas criminosos. As actividades criminosas nesta área têm impacto no crescimento socioeconómico do país e reforçam a necessidade de o Governo e os diferentes intervenientes da sociedade se capacitarem com urgência para combater estas práticas criminosas, com recursos humanos e tecnológicos adequados.

Na *Internet*, estudos como o "*Analysis of Mozambican Websites: How do they Protect their Users*", publicado em 2018, expõem as vulnerabilidades das páginas *Web* moçambicanas, e demostram como 32% de 240 páginas analisadas, a sua maioria da Administração Pública, não usam tecnologia adequada para a sua protecção contra os ataques cibernéticos.

b. Quadro legal: nacional, regional e continental

i. Nacional

Na área legal, é notório o esforço do país e do Governo na elaboração e aprovação de instrumentos normativos para atender aos desafios de cibersegurança. Neste contexto, destaca-se os seguintes instrumentos:

1. Regulamento de Controlo de Tráfego de Telecomunicações, Decreto n.º 75/2014, de 12 de Dezembro;
2. Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho;
3. Lei de Transacções Electrónicas, Lei n.º 3/2017, de 9 de Dezembro;
4. Regulamento do Quadro de Interoperabilidade de Governo Electrónico, Decreto n.º 67/2017, de 1 de Dezembro;
5. Política para a Sociedade da Informação, Resolução n.º 17/2018, de 21 de Junho;
6. Regulamento de Protecção do Consumidor do Serviço de Telecomunicações, Decreto n.º 44/2019, de 22 de Maio;
7. Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, Resolução n.º 5/2019, de 20 de Junho;
8. Regulamento de Segurança de Redes de Telecomunicações, Decreto n.º 62/2019, de 1 de Agosto;
9. Regulamento do Sistema de Certificação Digital de Moçambique, Decreto n.º 59/2019, de 1 de Dezembro;
10. Código Penal, Lei n.º 24/2019, de 24 de Dezembro ;
11. Regulamento do Domínio .mz, Decreto n.º 82/2020, de 10 de Setembro.

Em muitos países, a questão de segurança cibernética está estrategicamente enquadrada na defesa e segurança nacional, uma experiência de que se tirou proveito na elaboração da presente política e a sua estratégia, estabelecendo uma ponte entre a segurança nacional e a governação cibernética através do Conselho Nacional de Segurança Cibernética.

ii. Regional (SADC)

Em 2013, a Comunidade de Desenvolvimento da África Austral (SADC) desenvolveu uma Lei modelo para a protecção de dados no seio da organização, que serve de guia para as leis de protecção de dados a nível nacional. O modelo prevê o estabelecimento de autoridades nacionais de protecção de dados e também estabelece regras gerais de processamento de dados pessoais e deveres para controladores e processadores de dados, bem como direitos de titulares de dados.

iii. Continental (União Africana)

A globalização e a interconexão das redes de comunicações exigem soluções focadas na colaboração internacional, com destaque para a regional, que deve ser precisa, eficiente e eficaz.

Dada a complexidade da sociedade na Era digital e os desafios das TIC, é crucial levantar a questão de segurança cibernética a partir de uma perspectiva africana, onde apenas 20% dos países possuem legislação relacionada a segurança cibernética em vigor, designadamente:

a) alguns Estados têm disposições básicas de direito material e processual, mas não possuem regulamentos específicos de segurança cibernética;
b) outros possuem disposições substantivas e processuais parcialmente implementadas;
c) a maioria dos países não possui disposições legais específicas sobre crimes cibernéticos e evidências electrónicas;
d) nalguns casos, há projectos de Lei ou de emendas à legislação, mas o processo para a sua aprovação é moroso.

No caso de Moçambique, o país já ratificou a Convenção da União Africana sobre Segurança Cibernética e Protecção de Dados Pessoais, que representa um importante e significativo marco para a segurança cibernética, transacções electrónicas e protecção de dados pessoais.

A adaptação da legislação deve acompanhar o aprimoramento das capacidades da justiça criminal, desde o estabelecimento de unidades especializadas em investigação de crimes cibernéticos e computação forense, até ao fortalecimento da aplicação da lei e formação judicial, cooperação entre interagências, investigações financeiras, protecção à criança, cooperação público-privada e internacional.

Os governos não podem permanecer passivos face aos desafios relacionados com a matéria de segurança cibernética, visto que possuem a obrigação de proteger a sociedade, os activos de informação e as infra-estruturas críticas, e o cidadão.

Os ataques cibernéticos direccionados às economias africanas estão a aumentar rapidamente, não obstante existirem muitos sinais positivos e encorajadores de acções em curso com vista a combater o crime cibernético, visto que se tem elaborado

diversos planos, procedimentos e legislação sobre a segurança cibernética, envolvendo o sector público, privado, academia e a sociedade civil para fortalecer o cenário de segurança cibernética no continente africano.

iv. Tendências globais

A tendência internacional mostra o aumento de incidentes e ataques cibernéticos, em frequência, grau, número, qualidade e sofisticação dos ataques. É, no entanto, um ponto forte o facto de os governos e o sector privado africanos reconhecerem a necessidade de (i) investir na protecção de infra-estruturas críticas, (ii) estabelecer mecanismos e estruturas de coordenação da segurança cibernética, (iii) investir no desenvolvimento da capacidade técnica, e (iv) adoptar modelos de coordenação e cooperação em segurança cibernética para enfrentar o crescente número de ataques, ameaças e riscos cibernéticos.

As tecnologias digitais emergentes, consideradas como sendo aquelas ainda em desenvolvimento ou cujo desenvolvimento se perspectiva para os próximos anos e que se espera que venham a influenciar e/ou a condicionar, de forma disruptiva, duradoura e sistemática, a evolução futura da Sociedade e da Economia, constituem um conceito que congrega uma vasta diversidade de áreas tecnológicas e científicas. Estas também trazem elementos e dimensões acrescidas de segurança cibernética.

Desde 2020 que a Pandemia da COVID-19 está a ter um impacto negativo na saúde, na economia e outras áreas de desenvolvimento social e económico. Como parte da resposta global a esta pandemia a promoção do uso das TIC, em particular das tecnologias emergentes da computação em nuvem, *Internet* das Coisas (IoT), a Inteligência Artificial, BigData, robótica entre outros, conheceram um crescimento significativo nos países desenvolvidos.

Com o aumento da necessidade da realização de trabalho a partir de casa ou de forma remota, as TIC constituíram solução de eleição, e mostraram a sua grande utilidade em áreas como a telemedicina, teleducação, prestação de serviços digitais, reuniões por vídeo videoconferência, monitoria remota de instalações, de entre outras actividades no sector produtivo característicos da 4.ª Revolução Industrial. As ameaças à segurança de sistemas de *Internet*-das-Coisas (IoT) e de Inteligência Artificial, ampliaram a área de superfície para ataques e deslocaram os alvos de ataques cibernéticos de locais centralizados (o escritório) para locais distribuídos e em rede.

A economia digital está crescendo e os crimes cibernéticos estão igualmente aumentando, em todo o mundo, não sendo o nosso país uma excepção. Por isso, Moçambique tem muitos desafios na prevenção e combate aos crimes cibernéticos, sendo necessário o reforço na legislação, infra-estrutura, equipamentos e na capacitação de recursos humanos e institucional de modo a reforçar os conhecimentos sobre as medidas de segurança cibernética.

Os crimes cibernéticos têm uma dimensão transnacional podendo ocorrer num lugar e em pouco tempo se propagarem para todo o mundo, afectando não só uma região, mas todo o planeta. A título de exemplo pode-se referir os ataques do *ransomware* e outros *malwares*. Os crimes cibernéticos representam perigo significativo para as infra-estruturas de Tecnologias de Informação (TI), tendo este facto levado a União Internacional das Telecomunicações (UIT), nos princípios da década passada, a alertar para o aumento de ataques, que na altura afectavam cerca de 550 milhões de pessoas em todo o mundo, com prejuízos avaliados em 110 bilhões de dólares norte-americanos.

A implementação da PENSC poderá implicar, a médio e longo prazo, a necessidade da criação, revisão e actualização de alguns dos instrumentos normativos, tendo em conta a dinâmica do sector das TIC, sendo de destacar os Regulamentos de Segurança de Redes, Regulamento de Registo SIM CARDs, Regulamento de Construção e Operação de Centros de Dados, Regulamento de Computação em Nuvem, bem como o Regulamento de Protecção de Consumidores de Serviços e Produtos Digitais.

De acordo com *World Economic Fórum Global Risks Report* 2019, os ataques cibernéticos são um dos 10 principais riscos globais de maior preocupação para a próxima década. Segundo o documento, a fraude e roubo de dados digitais estão classificados na 4.ª posição e os ataques cibernéticos ocupam a 5.ª posição a nível Global, o seu custo potencial pode chegar a 90 triliões de dólares norte-americanos de impacto económico líquido, até 2030, se os esforços de segurança não acompanharem o crescimento da inter-conectividade. Embora os líderes governamentais e corporativos estejam profundamente engajados na promoção de estratégias eficazes de segurança cibernética e os gastos globais em segurança cibernética continuem aumentando, verifica-se que o número dos ataques cibernéticos atingiu o nível mais alto de todos os tempos em 2019.

A Política Nacional de Segurança Cibernética, aborda aspectos legais e tecnológicos que visam proteger pessoas (colectivas ou singulares) e bens, com destaque às infra-estruturas críticas de informação no espaço cibernético sob a responsabilidade de Moçambique.

c. Visão, Missão, objectivos, princípios orientadores e Pilares

Para responder aos desafios de segurança cibernética em Moçambique foi definida a visão, missão e objectivos específicos abaixo apresentados.

i. Visão

Uma nação com um espaço cibernético seguro, resiliente e uma sociedade consciencializada sobre as matérias de segurança cibernética.

ii. Missão

Criar e desenvolver uma capacidade institucional e operacional que garanta um ambiente seguro e atrativo no espaço cibernético.

iii. Objectivos

Objectivo Geral

Assegurar a protecção de Activos de Informação públicos e privados e suas Infra-estruturas Críticas no espaço cibernético.

Objectivos específicos

Os objectivos específicos são:

1. Estabelecer um mecanismo nacional de promoção de partilha, cooperação e coordenação em matérias de segurança cibernética;
2. Proteger as infra-estruturas críticas de informação;
3. Criar um quadro legal e técnico-operacional de segurança cibernética;
4. Proteger os activos de informação;
5. Desenvolver a capacidade de pesquisa e inovação em matéria de segurança cibernética;
6. Promover uma cultura nacional de segurança cibernética.

***d*. Princípios orientadores**

Os princípios orientadores da PENSC são:

1. **Princípio de Legalidade**: garantir que as medidas legislativas para o combate ao crime cibernético sejam harmonizadas a nível nacional e se considere como infracções os actos que afectam a privacidade e liberdades dos cidadãos, a integridade, disponibilidade e resiliência das infra-estruturas críticas e dos sistemas de informação conferindo segurança jurídica a nível nacional, regional e internacional.

2. **Princípio de Gestão de Riscos**: na planificação e desenvolvimento das TIC, há necessidade de desenvolver capacidades técnicas institucionais e operacionais para lidar com cenários de incerteza no espaço cibernético, através de abordagens preventivas e correctivas, com o objectivo de minimizar o impacto das mudanças, ameaças e riscos cibernéticos.

3. **Princípio de Responsabilidade**: todos os actores da PENSC têm o dever de cumprir as suas responsabilidades no âmbito da segurança cibernética e responder pelos seus actos.

4. **Princípio de Cooperação e Colaboração**: na implementação das iniciativas de TIC, todas as partes devem respeitar os mecanismos de cooperação e colaboração, a nível interno e internacional, de modo a garantir uma governação da *Internet* transparente e eficaz, em que todos os actores dão a sua contribuição. A cooperação e colaboração é, portanto, um dos mandamentos mais importantes da segurança cibernética, e deve nortear o funcionamento das Equipas de Resposta a Incidentes de Segurança Computacionais (CSIRT).

5. **Princípio de Inclusão**: este princípio procura assegurar que todos os cidadãos moçambicanos, independentemente do género, religião, raça, situação económica, opção política e sua localização, entre outros atributos, tenham acesso às TIC e possam utilizar o espaço cibernético de forma segura.

e. Pilares da Política

Os pilares que sustentam a PENSC são seis, a saber:

I. Liderança e Coordenação: estabelecer um Mecanismo Nacional de Promoção, Partilha, Cooperação e Coordenação em Matérias de Segurança Cibernética.

II. Protecção de Infra-estruturas Críticas de Informação (ICI): o objectivo deste pilar é a identificação e protecção das ICI e toda sua envolvente cobrindo sistemas, dispositivos, processos e pessoas, para garantir que não sejam afectadas, e, consequentemente, também a segurança territorial, a estabilidade política, económica e social do país, assim como a reputação das instituições e dos cidadãos. A responsabilidade de protecção destas infra-estruturas recai a todos os actores da PENSC, através de aplicação de medidas de detecção, prevenção e observância da legislação aplicável.

III. Protecção de Activos de Informação: o objectivo deste pilar é a protecção de informação e aplicações, através de estabelecimento de programas de certificação de qualidade e segurança das aplicações e infra-estruturas, mecanismos de controlo de acessos, estratégias de protecção da confidencialidade, integridade e disponibilidade da informação, regulamentos de protecção de informação, adopção de soluções tecnológicas de protecção e de resiliência de sistemas e Activos de Informação, assim como de realização de auditorias e avaliação dos níveis de maturidade no âmbito de segurança cibernética.

A informação constitui um importante recurso para o desenvolvimento, segurança e defesa das nações, e qualquer impedimento ao acesso ou destruição podem pôr em causa a confiança de cidadãos ou interesses particulares, inclusive a soberania de um país. Por isso, devem ser implementadas medidas contra situações de ameaças às liberdades individuais, aos dados pessoais e, em suma, à privacidade, confidencialidade e integridade de dados.

IV. Quadro Legal e Regulatório: o objectivo deste pilar é desenvolver um quadro legal e regulatório capaz de harmonizar as práticas a nível nacional, regional e internacional, simplificar e efectivar o combate a crimes cibernéticos, proporcionando segurança jurídica no ciberespaço. Nesta perspectiva, o quadro jurídico-administrativo deve ser melhorado para facilitar a actuação das autoridades, identificação, investigação, esclarecimento e aplicação de medidas em casos de contravenção.

V. Desenvolvimento de Capacidade, Pesquisa e Inovação: o objectivo deste pilar está focado em acções voltadas para a criação e fortalecimento das capacidades organizacionais, dos recursos humanos e tecnológicos, consciencialização, promoção da pesquisa e inovação. Para o alcance deste objectivo, devem ser desenvolvidos programas de formação técnica, capacitação, certificação, consciencialização, promoção de pesquisa e inovação, de modo que a sociedade, a academia, os sectores público e privado disponham dos recursos necessários para actuarem no ciberespaço.

VI. Cultura de Segurança Cibernética e Consciencialização: o objectivo é tornar o cidadão cada vez mais consciente de ameaças e riscos cibernéticos. Por isso, devem ser desenvolvidos programas de consciencialização para transmitir as boas práticas de uso das TIC, que possam contribuir para a redução de exposição a riscos de incidentes cibernéticos.

f. Factores Críticos de Sucesso

A implementação bem-sucedida da PENSC dependerá amplamente ou será influenciada pelos seguintes factores:

1. Liderança a alto nível: é fundamental uma liderança política ao mais alto nível, comprometida com a segurança cibernética nacional. Ela é assegurada pelo mecanismo de orientação política coordenado pelo Conselho Nacional de Segurança Cibernética. Portanto, a liderança política constitui o factor crítico principal para o sucesso da PNSC, porque cabe a ela garantir a sua coordenação, articulação, motivação e integração de esforços para a estratégia de implementação.

2. Capital humano: a implementação eficiente da segurança cibernética requer recursos humanos altamente qualificados em todos os sectores da sociedade. A capacidade das instituições do sector público e privado de obter e reter recursos humanos qualificados é, portanto, importante para manter e garantir uma forte abordagem de protecção contra ameaças cibernéticas, especialmente com operadores de Infraestrutura crítica, assim sendo é extremamente importante que o Governo invista na formação do capital humano.

3. Coordenação e colaboração: o Sincronismo das acções entre os diversos sectores deve ser assegurado, para que no final o conjunto de todas acções garantam a implementação efectiva. Vê-se vital este sincronismo na medida em que a garantia da segurança cibernética ser somente possível se houver acções transversais em todos os sectores. A natureza do espaço cibernético é sem fronteiras e complexa; isso implica que a gestão de riscos seja uma responsabilidade partilhada. Vários actores importantes além do governo de Moçambique, incluindo operadores de infra-estruturas críticas, sector público, sector privado, academia, sociedade civil e cidadãos, devem partilhar essa responsabilidade com base em colaboração harmoniosa. A colaboração internacional é essencial para garantir a presença de capacidade e mecanismos para lidar com ameaças cibernética sem fronteiras, além de fornecer assistência a aliados internacionais quando necessário. A capacidade de criar confiança e relacionamentos com os principais interessados (indústria, organizações internacionais de segurança cibernética e Estados soberanos) é importante devido ao facto de que as ameaças cibernéticas abrangerem várias jurisdições.

4. Monitoria: de forma a regular a implementação da PENSC é necessária uma monitorização constante das acções realizadas por todas partes envolvidas. A supervisão da conformidade de todas as principais partes interessadas e actores do sector público e privado fornece garantia para melhorar a maturidade de segurança cibernética do país. Isso requer esforço e iniciativa deliberada de cada parte interessada para cumprir com as suas obrigações. É necessária uma coordenação adequada dos esforços com o objectivo de realizar as actividades relacionadas com

segurança cibernética entre os sectores e garantir que soluções a nível nacional e soluções a nível sectorial sejam coordenadas.

Para o sucesso da implementação da presente estratégia, torna-se crucial a adopção de diretrizes emanadas por órgãos nacionais, regionais internacionais.

5. Financiamento: os recursos financeiros são uma importante componente da PENSC, sem a qual não será possível alcançar os objectivos pretendidos na sua plenitude. Trata-se de um factor crítico-chave que merecerá uma maior atenção na implementação da política, para que uma grave lacuna financeira não ponha em causa a soberania cibernética do país.

3. Estratégia de implementação

A presente estratégia tem um horizonte de 5 anos, e está alinhada com as cinco áreas transversais da Estratégia de Transformação Digital de África (2020-2030), concretamente no que concerne ao tema de segurança cibernética e protecção de dados pessoais.

Neste contexto, a PENSC é um importante instrumento orientador da governação, não só porque satisfaz os anseios dos moçambicanos no domínio cibernético, mas também porque conforma o país com uma das grandes preocupações de actualidade em todo o mundo, no âmbito da Sociedade Global da Informação.

a. Projectos/Iniciativas

Os projectos e iniciativas da estratégia de implementação da politica de segurança cibernética foram definidos em alinhamento com os pilares da PENSC, associando a cada um deles parte das vinte e cinco (25) iniciativas através das quais serão implementadas várias acções que concorrem para a materialização dos seus objectivos específicos.

i. Alinhamento entre os pilares, objectivos e Projectos/ Iniciativas

O quadro que se segue mostra o enquadramento das iniciativas, num total de 25, nos objectivos específicos e pilares da PENSC:

Tabela 1. Alinhamento entre os Pilares, Objectivos Específicos e Iniciativas

Pilares	Objectivos Específicos	Iniciativas	
Liderança e Coordenação	Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética	1	Estabelecer o Conselho Nacional de Segurança Cibernética (CNSC).
		2	Estabelecer a equipa central de Equipas de Resposta a Incidentes de Segurança Computacionais (CSIRT Nacional).
		3	Criar a Rede Nacional de CSIRT.
		4	Estabelecer o Centro Nacional de Operações de Segurança Cibernética (SOC Nacional).
		5	Criar o Observatório Nacional de Segurança Cibernética (ONSC).
Protecção de Infra-estruturas Críticas de Informação	Proteger as ICI	6	Mapear as ICI e identificar riscos e vulnerabilidades a ataques e outros incidentes cibernéticos.
		7	Desenvolver directrizes, instrumentos legais e regulatórios para a protecção de ICI .
		8	Estabelecer procedimentos de auditoria às ICI.
Quadro Legal e Regulatório	Criar o quadro legal de segurança cibernética	9	Rever e harmonizar o quadro legal.
		10	Reforçar o quadro legal sobre a segurança cibernética.
		11	Ratificar convenções internacionais sobre segurança cibernética.
		12	Assinar acordos de cooperação judiciária em matérias de cibercriminalidade.
		13	Assinar tratados internacionais sobre segurança cibernética.
		14	Promover e divulgar o quadro legal sobre segurança cibernética.
Protecção de Activos de Informação	Proteger os Activos de Informação	15	Estabelecer sistemas de mitigação e alerta sobre incidentes cibernéticos.
		16	Criar mecanismos de filtragem e remoção de conteúdos ilegais.
		17	Criar as equipas sectoriais de resposta a incidentes de segurança computacionais.
		18	Desenvolver programas de simulação dos incidentes de segurança cibernética.
		19	Desenvolver e implementar o sistema de certificação digital de Moçambique.
		20	Elaborar diretrizes, recomendações e manual de procedimentos sobre segurança Cibernética.
Desenvolvimento de Capacidade, Pesquisa e Inovação	Desenvolver a capacidade técnico-operacional e de pesquisa e inovação em matéria de segurança cibernética	21	Desenvolver a capacidade técnico-operacional de resposta a segurança cibernética no país .
		22	Promover pesquisas e desenvolvimento que busquem soluções inovadoras na área de segurança cibernética.
		23	Promover e estabelecer centros de formação de excelência em segurança cibernética.
		24	Estabelecer parcerias de colaboração técnica a nível local, regional e internacional na prevenção e no

Pilares	Objectivos Específicos	Iniciativas	
			combate ao crime cibernético.
Cultura de Segurança Cibernética e de Consciencializaçã	Desenvolver programas e mecanismos de Consciencialização Sobre os Riscos Associados ao Espaço Cibernético	25	Realizar programas de consciencialização sobre a segurança cibernética com enfoque na protecção da criança e outros grupos vulneráveis.

ii. Descrição de iniciativas, indicadores, metas e entregáveis

Na Tabela 2, é feito o resumo descritivo das iniciativas e a indicação dos respectivos entregáveis, que serão os indicadores de desempenho da estratégia. A responsabilidade, cronograma e custos de execução constam dos anexos que, além de prioridade, parcelam os orçamentos da estratégia pelo triénio 2021 a 2023.

Tabela 2. *Descrição das Iniciativas, indicadores, metas e entregáveis*

#	Iniciativa	Resultados						Impacto
1	**Criar Conselho Nacional de Segurança Cibernética (CNSC)** **Descrição:** O CNSC é um órgão de governação de segurança cibernética liderado ao mais alto nível do Estado.	1. Decreto que cria o CNSC; 2. CNSC em funcionamento; 3. Decreto que aprova o Regulamento de Gestão de Risco de Segurança Cibernética.						Fortalecimento expressivo de medidas e capacidade de defesa, ofensiva e resposta no espaço cibernético soberano. Tornando o país um alvo mais difícil de ser atingido por actores hostis cibernéticos.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Criado o Conselho Nacional de Segurança Cibernética.	**Meta**	1	-	-	-	-	
2	**Criar Centro Nacional de Resposta a Incidentes de Segurança Computacionais (CSIRT Nacional)** Descrição: O CSIRT Nacional será um órgão central de coordenação nacional de equipas de resposta a incidentes de segurança computacionais.	1. Documento de criação o CSIRT Nacional; 2. Outros instrumentos relacionados a politicas, estratégias, e mecanismos de funcionamento da rede nacional CSIRT.						Abordar as causas-raíz dos ataques a nível nacional, reduzindo a ocorrência de ataques repetidos às mesmas vítimas e sectores.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Criado o CSIRT Nacional	**Meta**	1	-	-	-	-	
3	**Criar Rede Nacional de CSIRT** Descrição: Esta iniciativa consiste na criação de CSIRTs sectoriais em cada sector que possa servir a todas as entidades que tenham aspectos comuns nas suas actividades. Inclui também o estabelecimento da Rede Nacional de CSIRTs, a ser coordenada pelo CSIRT Nacional.	1. Criados os CSIRTs sectoriais; 2. Estabelecida a Rede Nacional de CSIRTs de Moçambique liderada pelo CSIRT Nacional; 3. Estabelecido o Modelo de coordenação e outros instrumentos organizativos da Rede Nacional de CSIRTs; e 4- Criado o Centro de Pesquisa e Analise de trafego da *Internet* (CATI).						Maior proporção dos incidentes devem ser comunicadas às autoridades, levando a uma melhor compreensão da dimensão e escala das ameaças no espaço cibernético soberano.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Criados CSIRT sectoriais	**Meta**	1	3	2	2	2	
4	**Criar Centro Nacional de Operações de Segurança Cibernética (SOC)** Descrição: O Centro de Operações de Segurança Cibernética (SOC) será uma plataforma de prestação de serviços com capacidade de observar e identificar eventos de segurança cibernética, recolher e analisar informações, e tomar as necessárias	1. Decreto que cria o SOC Nacional; 2. Outros instrumentos organizativos do SOC Nacional.						Tratamento eficaz, eficiente e abrangente dos incidentes cibernéticos, fruto da criação do Centro Nacional de Segurança Cibernética (NCSC) como mecanismo centralizado de notificação e resposta a

#	Iniciativa	Resultados						Impacto
decisões.								incidentes e ameaças.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Estabelecido o Centro Nacional de Operações de Segurança Cibernética (SOC).	**Meta**	-	1	-	-	-	
5	**Criar Observatório Nacional de Segurança Cibernética (ONSC).**	1. Diploma Ministerial que cria ONSC; 2. Estabelecido e operacionalizado o SOC Nacional.						Capacidade técnica cibernética de vigilância e desarticulação precoce das estruturas e actividades cibernéticas de terroristas, impedindo a evolução da sua capacidade.
Descrição: O ONSC é uma plataforma nacional de recolha e actualização de informação estatísticas em matéria de Segurança Cibernética, alimentada pela Rede Nacional de CSIRTs.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Criada a Plataforma *web* do observatório Nacional de Segurança Cibernética.	**Meta**	-	1	-	-	-	
6	**Mapear as ICI, identificando os riscos e vulnerabilidades a ataques e incidentes cibernéticos**	1. Manual de identificação e avaliação das ICI; 2. Formulário de registo das ICI; 3. Identificação das ICI; 4. Base de dados das ICI; 5. Directriz de funcionamento de ICI no âmbito da segurança cibernética.						Conhecer o nível de segurança cibernética nas ICI e práticas proporcionais de segurança cibernética; e ter conhecimento especializado para desenvolver e aplicar a capacidade cibernética de defesa da soberania.
Descrição: Esta iniciativa visa identificar e mapear as ICI do país para a identificação de riscos e vulnerabilidades a ataques e incidentes cibernéticos.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Infra-estrutura Crítica de Informação mapeadas.	**Meta**	-	50 %	100%	-	-	
7	**Desenvolver directizes, instrumentos legais e regulatórios para protecção das ICI**	1. Elaborado o manual de procedimentos de segurança das ICI; 2. Estabelecido o mecanismo de monitoria, avaliação, auditoria e testagem regular das vulnerabilidades das ICI.						Maior capacidade cooperativa e de defesa das ICI.
Descrição: Esta iniciativa visa desenvolver instrumentos legais e normativos para melhorar a colaboração e protecção das ICI.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Criados Instrumentos legais e regulatórios para protecção das IC.	**Meta**		1	1			
8	**Criar procedimentos proteção e**	1. Criado mecanismos de protecção						Garantia da capacidade

#	Iniciativa	Resultados						Impacto
	de auditoria às ICI Descrição: O estabelecimento de procedimentos às ICI visa criar um mecanismo para garantir a observância de políticas e normas de gestão da segurança cibernética, através de auditorias sistemáticas e regulares às referidas infra-estruturas.	de contra os ataques cibernéticos ao serviço de nomes de domínios da *Internet*; 2. Criado mecanismos de protecção de contra ataques cibernéticos ao serviço de atribuição e gestão de recursos da *Internet*; 2. Criado o manual de auditoria às ICI.						técnica cibernética das ICI na gestão da segurança cibernética.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Elaborado o Manuel de procedimentos de auditoria às ICI.	**Meta**	-	1	-	-	-	
9	**Rever e harmonizar o quadro legal** Descrição: A revisão e harmonização visa acautelar que a legislação esteja actualizada e não dispersa, e que se aplique os mesmos princípios, regras, sanções sobre a segurança cibernética.	Instrumentos legais revistos e harmonizados.						Aumento dos casos julgados e intervenções dos órgãos policiais em crimes cibernéticos.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Instrumentos legais revistos e harmonizados.	**Meta**	-	-	-	1	1	
10	**Reforçar o quadro legal sobre segurança cibernética** Descrição: O reforço do quadro legal visa acautelar as novas formas de criminalidade digital, incluindo a aprovação de novos instrumentos normativos que protejam o espaço cibernético de actividades contrárias à ordem interna e internacional.	Lista de instrumentos normativos aprovados: 1. Elaborado a Lei de Protecção de Dados; 2. Elaborado a Lei do Crime Cibernético; 3. Elaborado o Regulamento de Desenvolvimento, Contratação, Hospedagem e Prestação de Serviços de Computação na Nuvem; 4. Elaborado o Regulamento de Construção e Operação de Centros de Dados no país.						Redução do número, a gravidade e o efeito dos ataques cibernéticos bem-sucedidos contra o espaço cibernético nacional como consequência da aplicação de normas de segurança cibernética.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Instrumentos normativos aprovados	**Meta**	-	-	-	1	1	
11	**Ratificar convenções internacionais sobre segurança cibernética**	Ratificadas convenções e tratados regionais e internacionais sobre segurança cibernética.						Consolidação do consenso internacional quanto aos benefícios

#	Iniciativa	Resultados						Impacto
	Descrição: A ratificação de convenções e tratados regionais e internacionais em matérias de segurança cibernética visa garantir que o país esteja preparado para cooperar em igualdade de circunstâncias com outros países no ciberespaço.							de um espaço cibernético livre, aberto, pacífico e seguro.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Convenções e tratados regionais e internacionais sobre segurança cibernética ratificados.	**Meta**	-	1	-	1	-	
12	**Assinar acordos de cooperação judiciária em matérias da cibercriminalidade**	Assinados os acordos.						Acordos multilaterais ampliados para a promoção de condutas lícitas e responsáveis por parte dos Estados. Oportunidades dos parceiros conhecerem as melhores formas de interação com o governo em assuntos de segurança cibernética.
	Descrição: Esta iniciativa visa municiar o país em matérias de instrumentos de cooperação judiciária para prevenir e combater o crime cibernético aplicando o principio da dupla responsabilidade.							
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Acordos assinados os acordos.	**Meta**	-	1	1	1	-	
13	**Assinar tratados internacionais sobre segurança cibernética**	Assinados os tratados internacionais sobre segurança cibernética.						Fortalecimento da colaboração internacional, reduzindo as ameaças cibernéticas ao país e aos seus interesses no exterior; e Consolidação de redes de intercâmbio de informações com nossos parceiros internacionais.
	Descrição: Esta iniciativa visa que o nosso país com outros adoptem princípios e regras que promovam e combatam o cibercrime.							
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Tratados internacionais sobre segurança cibernética assinados	**Meta**	-	1	-	-	1	
14	**Promover e divulgar o quadro legal sobre segurança cibernética**	Elaborado e implementado o plano de promoção e divulgação.						Contribuir para maior consciencialização dos aspectos de segurança cibernética, fortalecendo a defesa do país no geral e o cidadão em particular.
	Descrição: Esta iniciativa concorre para a promoção de um ambiente de convivência sã no espaço cibernético para que os cidadãos passam a ter							

#	Iniciativa	Resultados						Impacto
consciência sobre os seus direitos, deveres e responsabilidades no espeço cibernético.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Número de campanhas de consciencialização sobre direitos, deveres e responsabilidades no espaço cibernético realizadas.	**Meta**	-	1	1	-	-	
15	**Estabelecer sistemas de mitigação e alerta sobre incidentes cibernéticos**	Sistemas de mitigação e alerta em funcionamento nas ICI e Activos de Informação.						O governo e as forças armadas terem acesso a especialistas cibernéticos capazes de preservar a segurança e a resiliência do espaço cibernético.
Descrição: Esta iniciativa visa criar sistemas de alerta sobre os incidentes cibernéticos em todas as ICI e Activos de Informação.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Estabelecido os sistemas de mitigação e alerta e em funcionamento nas ICI e Activos de Informação.	**Meta**	-	25 %	50%	100%	-	
16	**Criar mecanismo de filtragem e remoção de conteúdos ilegais**	Mecanismo de filtragem e remoção de conteúdos ilegais.						Bloqueio de uma proporção maior de ataque cibernéticos e a protecção de artefactos técnicos associados a ataques e exploração cibernética.
Descrição: O mecanismo de filtragem e remoção de conteúdos ilegais visa preservar os valores culturais e religiosos da sociedade, bem como proteger os direitos de propriedade intelectual e a integridade moral de pessoas colectivas e singulares.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Estabelecido o Mecanismo de filtragem e remoção de conteúdos ilegais.	**Meta**	-	1	-	-	-	
17	**Criar programas de simulação de incidentes cibernéticos**	1. Implementado um Sistema de simulação de incidentes cibernéticos. 2. Base de dados de testes sobre incidentes cibernéticos em Activo de Informação.						Aumento da capacidade e das competências tanto dos órgãos policiais especializados , dos técnicos e do cidadão no geral em matéria de protecção contra incidentes cibernéticos.
Descrição: Os programas de simulação de incidentes cibernéticos visam testar os sistemas de protecção contra incidentes cibernéticos.								
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Programas de simulação de incidentes cibernéticos realizados.	**Meta**	-	1	1	1	1	

#	Iniciativa	Resultados						Impacto
18	**Desenvolver e implementar o sistema de certificação digital de Moçambique** Descrição: Estabelecer os fundamentos técnicos e metodológicos do sistema de certificação digital baseado em criptografia de Chaves públicas e privadas.	1- Instalado o sistema de certificação digital de Moçambique; 2- Acreditados agentes do sistema de certificação digital.						Melhoria na integridade, autenticidade e segurança na tramitação de documentos oficias e na comunicação entre várias entidades.
	Indicador:	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Sistema de certificação digital instalado e funcional.	**Meta**		1	3	5	10	
19	**Elaborar diretrizes, recomendações e Manual de procedimentos sobre segurança Cibernética** Descrição: Elaborar diretrizes, recomendações e Manual de procedimentos que ajudem na melhoria da protecção dos sistemas e activos de informação.	1- Elaborado diretrizes para adopção de "*security by design*" nos sistemas e infra-estruturas de TI nacionais. 2- Elaborado recomendações de segurança para centros de dados. 3- Elaborado recomendações de segurança cibernética para computação na Nuvem.						Melhoria na adopção de medidas de segurança cibernética na fase de desenho e implementação de sistemas e infra-estruturas de TI a nível nacional concorrendo para a melhoria do ambiente de segurança cibernética.
	Indicador:	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	3 instrumentos orientadores elaborados.	**Meta**				1	2	
20	**Desenvolver capacidade técnico-profissional em matéria de resposta a incidentes cibernéticos** **Descrição**: O desenvolvimento de capacidade tecno-operacional em matéria de resposta a incidentes cibernéticos visa criar capacidades técnicas de prontidão aos profissionais responsáveis por forma a garantir a segurança das ICI para responder aos incidentes cibernéticos.	1. Estudo sobre capacidade da Administração Pública em recursos humanos; 2. Programas de desenvolvimento de competências cibernéticas; 3. Revisão dos currículos do sistema nacional da educação em matéria de segurança cibernética.						O governo e as forças armadas terem acesso a especialistas cibernéticos capazes de preservar a segurança e a resiliência do espaço cibernético; e A segurança cibernética ser ensinada efectivamente como parte integrante dos cursos relacionados no sistema de ensino, desde o ensino primário até a pós-graduação.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Graduados dos cursos técnico-profissionais na área de segurança cibernética	**Meta**	-	-	-	-	150	
21	**Promover pesquisas para soluções inovadoras na área de segurança cibernética**	1. Revista a agenda nacional de investigação e elaboradas as directrizes para a criação de centros						Aumento da capacidade de pesquisa e inovação em

#	Iniciativa	Resultados						Impacto
	Descrição: Esta iniciativa visa reforçar a agenda nacional de investigação de modo a focalizar a área de segurança cibernética, incluindo programa de incentivos fiscais para empresas que promovem soluções inovadoras em matéria de segurança cibernética.	de pesquisa; 2. Identificados os modelos para a realização de competições de soluções inovadoras em segurança cibernética. 3. Incentivar estudos para análise e implementação segurança cibernética no âmbito das tecnologias emergentes.						segurança cibernética, trazendo soluções inovadoras locais.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Número de pesquisas para soluções inovadoras na área de segurança cibernética realizadas.	**Meta**	-	1	1	-	1	
22	**Promover e estabelecer centros de formação de excelência em segurança cibernética** Descrição: Esta iniciativa visa alimentar o Estado, o governo e o mercado nacional em geral com técnicos de excelência altamente qualificados em matérias de segurança cibernética nos seus vários domínios. Prevê estabelecer pelo menos um centro de excelência por região no país.	1. Estabelecido centros de excelência em segurança cibernética; 2. Integrados cursos de segurança cibernética a nível de graduação, pôs-graduação, mestrado e Doutoramento a nível Nacional; 3. Formados 20 técnicos por províncias em matérias de segurança cibernética.						Aumento de especialistas de excelência em segurança cibernética concorrendo para melhoria da segurança cibernética no país.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Número de centros de formação de excelência em segurança cibernética.	**Meta**			1	1	1	
23	**Estabelecer parcerias de colaboração técnica a nível local, regional e internacional para a prevenção e combate ao crime cibernético** Descrição: As parcerias de colaboração técnico-profissional visam promover a troca de experiências a nível nacional, regional e internacional em matéria de segurança cibernética e a elevação da capacidade local para lidar com ameaças cibernéticas.	1. Acordos de parcerias locais, regionais e internacionais; 2. Centros de formação e pesquisa em segurança cibernética internacionais.						Consolidação de redes de intercâmbio de informações com parceiros internacionais e acordos multilaterais ampliados para a promoção de condutas lícitas e responsáveis por parte dos Estados.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Acordos de parcerias estabelecidos	**Meta**	-	1	1	1	-	

#	Iniciativa	Resultados						Impacto
24	**Realizar inquéritos nacionais de avaliação do nível de consciencialização dos sectores público e privado e da sociedade em geral em segurança cibernética** Descrição: Os inquéritos visam avaliar o nível de consciencialização dos sectores público e privado, bem como a sociedade em geral, em matéria de segurança cibernética, para a definição de acções de consciencialização que se julgarem necessárias.	1. Resultados do inquérito partilhados e divulgados; 2. Actualizado o ONSC.						Conhecer o nível de risco e do estágio em segurança cibernética em todos os sectores.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Inquéritos nacionais realizados	**Meta**	1	-	1	-	1	
25	**Desenvolver programas de Consciencialização sobre os Riscos Associados ao uso do Espaço Cibernético** Descrição: Os programas de consciencialização visam fundamentalmente criar uma cultura de segurança cibernética aos cidadãos, para que a *Internet* seja um espaço social, económico e cultural onde todos possam estar, trabalhar e conviver em harmonia.	1. Desenvolver campanhas de sensibilização sobre segurança cibernética; 2. Criar cartilhas de educação sobre segurança cibernética; 3. Promover fóruns e conferências sobre segurança cibernética; 4. Consciencializados 100 pessoas por província em matérias de segurança cibernética.						Maior capacidade de protecção em ataques de engenharia social e registo de melhorias na cultura de segurança cibernética no país, fruto da maior conscientização das organizações e da população sobre os níveis de risco cibernético e as medidas de higiene cibernética que devem tomar para geri-los.
	Indicador	**Período**	**2021**	**2022**	**2023**	**2024**	**2025**	
	Campanhas de consciencialização sobre os riscos associados ao uso do espaço cibernético realizados.	**Meta**	-	1	1	1	1	

b. Coordenação da Segurança Cibernética

A coordenação da segurança cibernética será assegurada pelo Conselho Nacional de Segurança Cibernética (CNSC), presidido pelo Ministro que superintende a área de Tecnologias de Informação e Comunicação.

i. Composição do Conselho Nacional de Segurança Cibernética (CNSC)

O Conselho Nacional de Segurança Cibernética tem a seguinte composição:

1. Representantes dos sectores ou entidades responsáveis pelas áreas de:

a) Defesa;
b) Ordem, segurança e tranquilidades públicas;
c) Tecnologias de Informação e Comunicação;
d) Justiça;
e) Comunicações;
f) Economia e Finanças;
g) Educação;
h) Saúde;
i) Género e Criança;
j) Energia;
k) Entidade reguladora de TIC;
l) Entidade reguladora das comunicações;
m) CSIRT nacional;
n) Secretariado Técnico.

2. Membros convidados para questões de consulta:

a) Representante da Academia;
b) Representante do Sector Privado;
c) Representante da Sociedade Civil.

A representação do sector empresarial, da academia e sociedade civil no CNSC através das respectivas associações confere ao órgão a natureza democrática porque garante a heterogeneidade na governação cibernética.

O Conselho Nacional de Segurança Cibernética será assessorado pelo secretariado técnico sob a responsabilidade do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) IP. O secretariado técnico assegura a componente e qualidade técnica do CNSC, e será constituído por um comité colegial englobando técnicos especialistas de outras instituições.

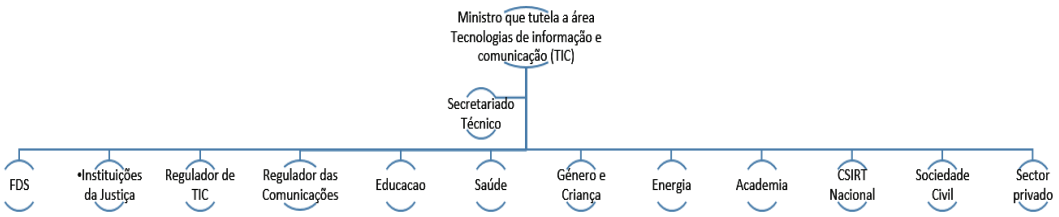

Figura 1. Estrutura do Conselho Nacional de Segurança Cibernética

ii. Papel do Conselho Nacional de Segurança Cibernética (CNSC)

Cabe ao Conselho Nacional de Segurança Cibernética (CNSC) a responsabilidade de garantir o alinhamento de políticas, estratégias e outros documentos orientadores da governação digital, a saber:

1. Assegurar a actualização da PENSC;
2. Garantir o desenvolvimento das normas que assegurem um quadro legal de segurança cibernética adequado à realidade nacional;
3. Atestar o desenvolvimento de metodologias, normas e outros instrumentos que assegurem soluções coerentes e uniformes para segurança cibernética;
4. Avaliar os riscos da estratégia e propor soluções para a sua eliminação ou mitigação;
5. Identificar as ICI e acções que visem garantir a sua protecção;
6. Avaliar o estado nacional de segurança cibernética, determinar as necessidades prioritárias e assegurar as respostas apropriadas para cada caso;
7. Acompanhar o progresso de implementação da PENSC;
8. Coordenar as actividades no âmbito da segurança cibernética;
9. Garantir acção conjunta contra crimes cibernéticos;
10. Garantir o desenvolvimento e actualização do Observatório Nacional de Segurança Cibernética, cuja informação deve permitir aferir o nível de segurança cibernética do país;
11. Garantir a consciencialização das instituições e dos cidadãos em matéria de segurança cibernética, assim como o estabelecimento de mecanismos de prevenção, detecção, monitoria e resolução dos crimes e incidentes de natureza cibernética.

O CNSC será apoiado por um secretariado executivo, que garantirá os aspectos técnicos, administrativos e logísticos de implementação da estratégia e funcionamento do Conselho.

Competirá ao secretariado fazer análise técnica e científica das matérias de segurança cibernética a submeter a CNSC, nomeadamente:

1. Propostas legislativas e regulatórias;
2. Propostas de mecanismos de coordenação interinstitucional;
3. Propostas em matérias de cooperação regional e internacional;
4. Medidas que visem garantir a segurança das comunicações e dos cidadãos no espaço cibernética nacional;
5. Medidas que garantam a protecção efectiva de dados pessoais e da privacidade;
6. Medidas que garantam a integridade e segurança das redes de comunicações públicas e dos serviços acessíveis ao público, incluindo as interligações nacionais e internacionais;
7. Medidas que garantam a coordenação das equipas de resposta a incidentes cibernéticos.
8. Promover e encorajar parcerias público-privada sobre assuntos relacionadas com a segurança cibernética no país;
9. Promoção de debates e pesquisas sobre a segurança cibernética;
10. Desenvolvimento de planos curriculares em segurança cibernética;
11. Aconselhamento sobre produtos e serviços essenciais sobre a protecção de Infra-estruturas de Tecnologias de Informação (TI);
12. Desenvolvimento de estratégias e arquitecturas de gestão de riscos cibernéticos na prestação dos vários serviços;
13. Soluções para a mitigação de vulnerabilidades cibernéticas; e
14. Acções de sensibilização pública sobre a segurança cibernética.

O Ministro que superentende a área de Tecnologias de Informação e Comunicação, apoiado tecnicamente pelo Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), a Autoridade Nacional de Segurança Cibernética, é responsável pelo funcionamento do Secretariado Executivo do Conselho Nacional de Segurança Cibernética (CNSC).

iii. Papel dos Intervenientes

Tabela 3. *Intervenientes e seus papéis*

#	Interveniente	Papel
1	**O Ministério que superentende a área de Tecnologias de Informação e Comunicação**	Através do Regulador para a área de TIC, o **INTIC, IP,** assume: 1- O papel da entidade responsável para implementação da presente estratégia que visa a melhoria do ambiente de segurança cibernética e tem a responsabilidade de desenvolver e propor um quadro legal para a implementação e Monitoria da presente estratégia. 2- Assegurar o cumprimento das acções e objectivos definidos na estratégia. 3- Criar um mecanismo de coordenação dos diferentes sectores envolvidos na unidade com vista ao alinhamento eficaz das acções e resultados esperados. 4- Definir e encontrar alternativas de financiamento das actividades relativas a implementação da estratégia. 5. O papel de incentivar o desenvolvimento de aplicações e sistemas de informação adoptando os princípios de *"security by design"*. 6- Monitorar o cumprimento dos prazos de cada uma das acções no âmbito da estratégia e assegurar que nenhum destes prazos são extrapolados.
2	**O Ministério que superentende a área das Comunicações**	Através do Regulador para a área das comunicações, o **INCM**, assume: . 1. O papel da entidade responsável pela promoção da cultura de segurança cibernética na área das telecomunicações, alinhadas com a presente estratégia, em estrita colaboração com o regulador de TICs. . 2. De regular com excelência os sectores postal e de telecomunicações para o desenvolvimento de moçambique observando as medidas de segurança cibernética em toda sua extensão. . 3. O papel de incentivar o desenvolvimento de infra-estruturas de banda larga e a massificação da utilização das tecnologias de informação e comunicação adoptando os princípios de *"security by design"*. . *4.* Criar um mecanismo de coordenação dos diferentes actores na área das telecomunicações, com vista a melhorar o ambiente de segurança cibernética no sector em particular e no país no geral. . *5.* Monitorar e fiscalizar o cumprimento e adopção das medidas de segurança cibernética no sector. . *6.* Dinamizar o processo de criação do CSIRT do sector das telecomunicações.
3	**O Ministério que superentende a área da Economia e Finanças**	O Ministério desempenha um papel preponderante no combate ao crime cibernético visto que este sector é o mais apetecível a crimes cibernéticos. Neste âmbito, assume: . 1. O papel da entidade responsável pela promoção da cultura de segurança cibernética na área financeira, alinhadas com a presente estratégia, em estrita colaboração com o regulador de TICs. . 2. De regular com excelência o sector económico e financeiro para o desenvolvimento de Moçambique observando as medidas de segurança cibernética em toda sua extensão. . 3. O papel de incentivar o desenvolvimento inclusivo do sector financeiro adoptando os princípios de *"security by design"*. . *4.* Criar um mecanismo de coordenação dos diferentes actores na área financeira e económica, com vista a melhorar o ambiente de segurança cibernética no sector em particular e no país no geral.

#	Interveniente	Papel
		5. Monitorar e fiscalizar o cumprimento e adopção das medidas de segurança cibernética no sector. *6.* O Banco de Moçambique deve dinamizar o processo de criação do CSIRT do sector financeiro. 7. Sem prejuízo da legislação especial o Banco de Moçambique deve emitir normas que estabeleçam garantias de segurança de todos os pagamentos efectuados por qualquer outro portador que utilizar um instrumento de pagamento electrónico. 8. O Banco de Moçambique, no âmbito das suas actividades de supervisão e fiscalização e auditorias as entidades supervisionadas, deve supervisionar, fiscalizar e auditar a implementação de medidas de segurança cibernéticas. 9. O Instituto de Supervisão de seguros de Moçambique (ISSM) no âmbito das suas actividades de supervisão, fiscalização e auditoria as entidades supervisionadas, deve supervisionar, fiscalizar e auditar a implementação de medidas de segurança cibernéticas. 10. O ISSM deve dinamizar o processo de criação do CSIRT do sector de seguros.
4	**CSIRT Nacional**	O CSIRT Nacional, na qualidade do órgão nacional de coordenação das equipes de resposta a incidentes cibernéticos tem no seu papel as seguintes responsabilidades: 1. Coordenar as acções de resposta a incidentes de segurança e ser o ponto central de notificações a nível nacional e internacional. 2. Servir de elo de ligação entre as redes nacionais de CSIRT e o CNSC. 3. Criar e manter o observatório nacional de segurança Cibernética. 4. Garantir a partilha de informação com vista a mitigação de crimes cibernéticos em Moçambique. 5. Motivar e garantir a criação de CSIRTs sectoriais . 6. Criar o Centro de Pesquisa e Análise de Tráfego da *Internet* (CATI).
5	**O Ministério que superintende a área da Justiça**	Desempenha um papel preponderante sendo o órgão do Governo que interage com os restantes da Administração da Justiça. Funções principais: 1. Coordenar os órgãos de Administração da Justiça no âmbito da segurança cibernética. 2. Delinear estratégias de respostas aos organismos internacionais sobre segurança cibernética. 3. Assessorar juridicamente ao Governo em matérias de segurança cibernética em coordenação com o Instituto Nacional de Tecnologias de Informação e Comunicação. 4. Adoptar técnicas e conhecimentos para recolha, preservação e análise de evidências de crimes cibernéticos. 5. Incentivar dentro dos órgãos judiciários, a adopção de técnicas e ferramentas que auxiliem na instrução dos processos por infração de crimes cibernéticos.
7	**O Ministério que superentende a área de Ordem e Segurança Pública**	Na qualidade das forças de lei e ordem, devem desenvolver capacidades de recolha, preservação e investigação de evidências de crimes cibernéticos. Funções principais: Desenvolver planos de formação para todas unidades policias conferindo maior capacidade para entender e investigar crimes cibernéticos.

#	Interveniente	Papel
		1.Estabelecer laboratório de análise forense para recolha e análise de evidências electrónicas sobre crimes cibernéticos. 2. Assessorar as entidades jurídicas no processo de criminalização em casos de violação ou crimes cibernéticos.
8	**O Ministério que superentende a área de Defesa e Segurança (FDS)**	As Forças de Defesa e Segurança no seu papel no quadro da segurança cibernética devem garantir: 1. A elaboração e implementação de uma estratégia de ciberdefesa. 2. Estabelecer o CSIRT da Defesa. 3. Desenvolver e consolidar a capacidade de ciberdefesa no país. 4. Garantir a complementaridade da presente estratégia com as acções de ciberdesefa.
9	**O Ministério que superentende a área da Saúde**	Desempenha um papel preponderante na definição das políticas e estratégias de uso de TIC na saúde e tem como principais funções: 1.Garantir a implementação de programas de segurança cibernética na saúde. 2.Promover o processo de formação inicial, continua e a distância a matéria de segurança cibernética dos profissionais da saúde. 3.Desenvolver valores e atitudes que promovam a cultura de protecção de dados pessoais na área da saúde. 4.O Ministério da saúde no âmbito das suas actividades de supervisão e fiscalização e auditorias as entidades supervisionadas, deve supervisionar, fiscalizar e auditar a implementação de medidas de segurança cibernéticas na área da saúde. 5.Promover a criação do CSIRT sectorial da área da saúde.
10	**O Ministério que superentende a área da Educação e de Desenvolvimento Humano**	Desempenha um papel preponderante na definição das normas de planificação curricular e na definição de políticas e estratégias da educação e desenvolvimento humano. Funções Principais: 1.Garantir a implementação de programas de ensino escolar relacionadas a segurança cibernética, 2.Promover o processo de formação inicial, continua e a distância a matéria de segurança cibernética; 3.Desenvolver valores e atitudes que promovam a cultura de segurança cibernética. 4.O Ministério da Educação e Desenvolvimento Humano, no âmbito das suas actividades de supervisão e fiscalização e auditorias as entidades supervisionadas, deve supervisionar, fiscalizar e auditar a implementação de medidas de segurança cibernéticas. 5.Promover a criação do CSIRT sectorial da área de Educação e Desenvolvimento Humano.
11	**O Ministério que superentende a área da Energia**	Entidade responsável pela promoção no desenvolvimento e aproveitamento do potencial dos recursos minerais e energéticos e respectivas infra-estruturas. Funções Principais: 1- Proteger as infra-estruturas físicas e virtuais contra as ameaças

#	Interveniente	Papel
		cibernéticas. 2- Através do Regulador de Energia (ARENE) deve incentivar a criação do CSIRT do sector. 3- Através da ARENE emitir directrizes de segurança cibernética para os seus constituintes. 4- A ARENE, no âmbito das suas actividades de supervisão e fiscalização e auditorias as entidades supervisionadas, deve supervisionar, fiscalizar e auditar a implementação de medidas de segurança cibernéticas.
12	**O Ministério que superentende a área do Género e Criança**	Desempenha um papel preponderante na elaboração de propostas de politicas, estratégias, programas e legislação em prol da igualdade de género, empoderamento da mulher e protecção da criança. Funções principais: 1. Implementar programas contra a violação dos direitos das crianças no ciberespaço. 2. Promover Planos e iniciativas para a prevenção da criança no ciberespaço. 3. Criar e divulgar plataformas para denúncia e protecção de crimes e incidentes cibernéticos no espaço cibernético.
13	**Academia**	A academia desempenha um papel preponderante, para a criação de um ambiente cibernético seguro, cabendo a ela: 1. Promover debates no âmbito de segurança cibernética. 2. Encorajar as pesquisas e desenvolvimento para mitigar ou solucionar problemas de segurança cibernética. 3. Desenvolver planos curriculares para a formação de futuros profissionais no âmbito da segurança cibernética.
14	**Sector Privado**	O sector privado é um parceiro chave na implementação das soluções com vista a mitigação dos riscos de segurança cibernética. As suas funções são: 1. Aconselhar sobre produtos e serviços essências para assegurar a protecção das suas infra-estruturas. 2. Fornecer estratégias e arquitecturas de segurança, operações e abordagens de gestão de risco dos serviços. **3.** Fornecer soluções para a mitigação de vulnerabilidade de segurança.
15	**Sociedade Civil**	A sociedade civil desempenha um papel de relevo, cabendo a ela: 1. Alimentar o ecossistema das ameaças cibernéticas mais comuns. **2.** Sensibilizar e disseminar acções com vista a precaução e mitigação de riscos cibernéticos.

iv. Mecanismo de Coordenação da Rede Nacional de CSIRTs

O CSIRT Nacional, a funcionar no Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC, IP) e com assento no Conselho Nacional de Segurança Cibernética, actua oficiosamente e quando solicitado por um dos membros da Rede Nacional de CSIRTs, como o centro de coordenação e canalização de informações técnica e estratégicas servindo de elo de ligação entre a Rede Nacional de CSIRTs e o Conselho Nacional de Segurança Cibernética.

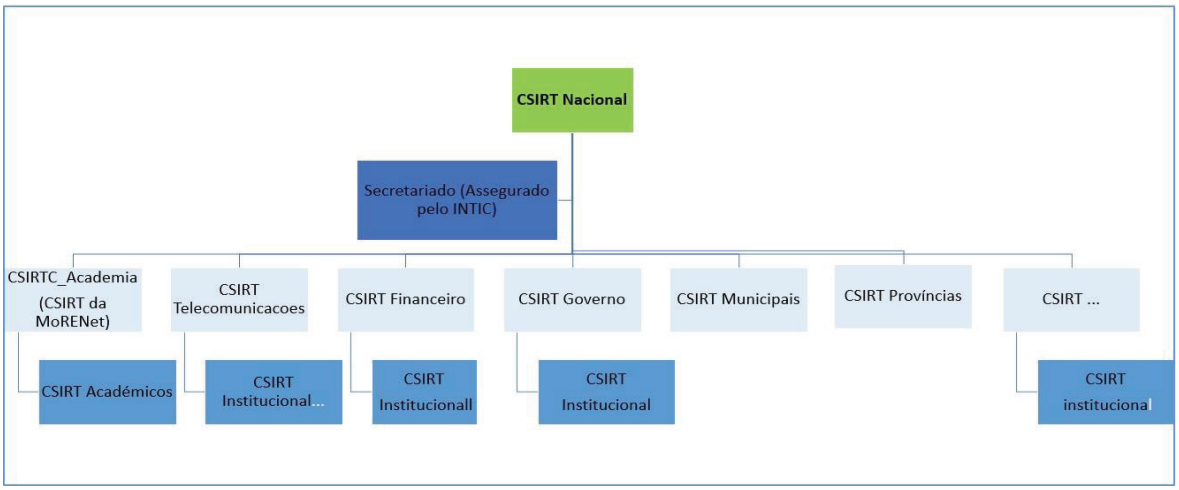

Figura 2. *Estrutura da Rede Nacional de CSIRTs*

Para além das infra-estruturas críticas de informação e comunicação, os sectores da Telecomunicações, energia, finanças, banca, saúde, água, seguros, Governos províncias e municipais representam sectores chaves e são chamados a criar com a maior brevidade, os CSIRT sectoriais e adoptar mediadas arrojadas de segurança cibernética. Os demais sectores da economia e segmentos da nossa sociedade, devem criar igualmente CSIRTs nos respectivos sectores, segmentos sociais e dinamizar o processo de criação de equipes de prevenção e combate (resposta) a incidentes cibernéticos a nível sectorial e institucional.

Os CSIRTs sectoriais, no âmbito das suas acções de prevenção e combate (resposta) aos abusos no espaço cibernético e ao cibercrime, actuam como elo de ligação entre o CSIRT nacional e as equipes de resposta a incidentes cibernéticos nas instituições, os CSIRTs institucionais.

As equipes de resposta a incidentes cibernéticos institucionais devem velar pela segurança cibernética nas respectivas instituições prestando serviços de assistência ao utilizador final, o cidadão e as instituições, e devem colaborar com os CSIRTs dos respectivos sectores.

Sendo o sector financeiro o mais apetecível para crimes cibernéticos, especial atenção deve ser conferida a este sector encorajando-se a criação e desenvolvimento do CSIRT deste sector.

Sectores chaves do governo e mais apetecíveis a crimes cibernéticos tais como ministério das finanças, saúde e energia são encorajados a adoptar medidas arrojadas no combate e resiliência ao cibercrime.

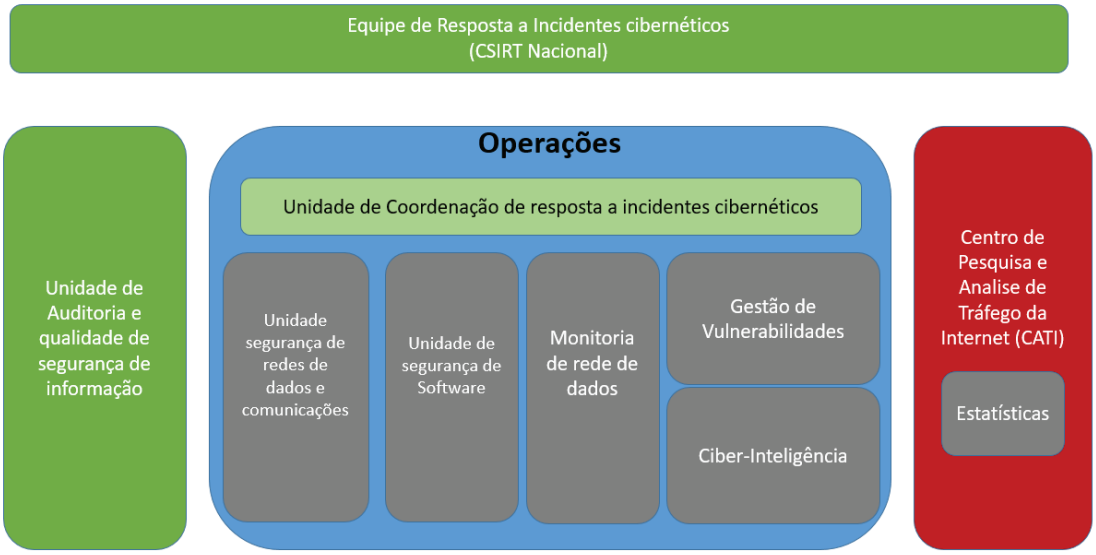

Figura 3. *Estrutura funcional do CSIRT Nacional*

b. Monitoria e Avaliação

Para que os responsáveis pela implementação das iniciativas mantenham a consistência na implementação dos objectivos e acções previstas no plano estratégico é essencial um mecanismo de Monitoria e Avaliação para controlar a eficácia e eficiência e para apreciar o impacto das iniciativas programadas.

A monitoria sendo um processo contínuo de recolha e análise de informações será realizada trimestralmente com a finalidade de aferir a qualidade da execução das iniciativas da estratégia, através da recolha de dados juntos dos responsáveis pela implementação sobre o progresso e dificuldades enfrentados na obtenção de resultados esperados desde o início, de modo a permitir que as partes tomem todas as medidas correctivas necessárias.

Avaliação será feita em duas etapas sendo avaliação intercalar e avaliação final. Na avaliação intercalar será feita uma análise das diferenças entre os resultados alcançados e os esperados, de modo a permitir que as mudanças necessárias sejam feitas, incluindo o cronograma de actividades reajustado para a segunda etapa do período da estratégia. Na avaliação final deve-se realizar uma pesquisa, com a finalidade de monitorar o nível de maturidade da cibersegurança no Sector Público, Sector Privado, Academia e na Sociedade Civil, de modo a permitir a tirada de lições e a preparação do progresso para o futuro plano nacional de segurança cibernética.

A monitoria e avaliação da PENSC será realizada com base num plano, o qual incidirá sobre:

1. Metas a nível das instituições governamentais e outras partes interessadas;
2. Resultados esperados e recursos necessários envolvidos;
3. Indicadores de desempenho, impacto e execução.

O plano de monitoria e avaliação deverá iniciar até três meses após a aprovação da estratégia.

Trimestralmente deve-se produzir relatórios com os indicadores compilados e avaliados, as tendências e as mudanças necessárias a serem implementadas em relação a informação e as actividades.

Os relatórios sectoriais são geralmente produzidos pelos diferentes órgãos, directamente, envolvidos na implementação da estratégia. Os CSIRT sectoriais devem produzir os relatórios de monitoria e avaliação trimestral e enviar para o CSIRT nacional, que por sua vez vai compilar e sistematizar os dados e produzir o relatório nacional.

Os relatórios anuais são produzidos a partir de relatórios produzidos pelos CSIRT sectoriais, num modelo padrão para facilitar a sua combinação.

i. Ciclo de monitoria

A monitoria e avaliação é composto pelo ciclo de monitoria que apresenta os momentos contínuos de interacção da estrutura de implementação das iniciativas, conforme mostra a Figura 4.

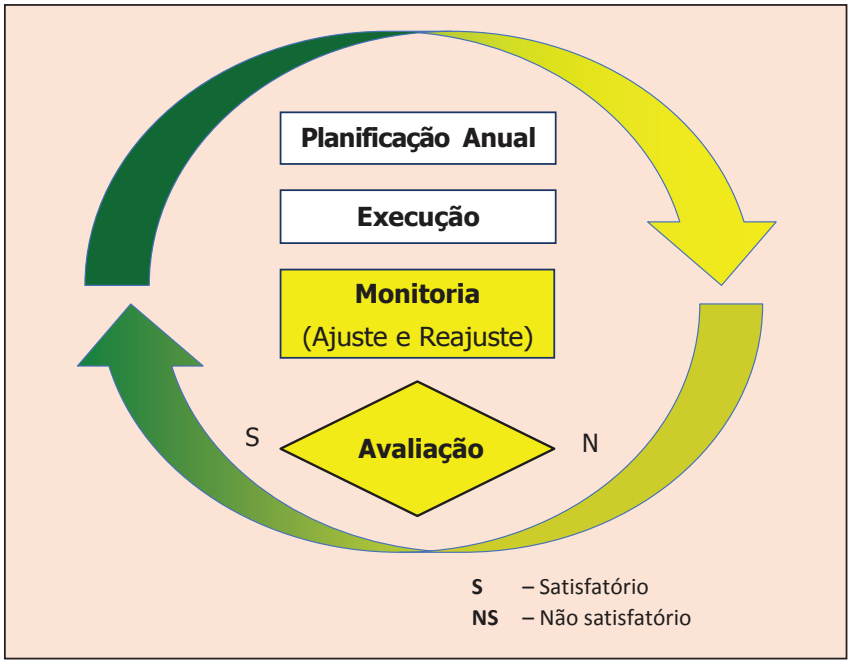

Figura 4. *Ciclo de Monitoria da PENSC*

Anualmente, O Conselho Nacional de Segurança Cibernética vai ter uma sessão de trabalho específico dedicada a aprovação do relatório anual, plano e orçamento das actividades a serem realizadas no ano seguinte, relativa a implementação de cada uma das vinte e cinco (25) iniciativas e definir as metas a atingir, alinhadas ao Plano Estratégico. Trimestralmente, serão realizadas sessões do CSIRT Nacional relativa a monitorização e a avaliação do grau de progresso da implementação das iniciativas, e para a aferir não só o grau de cumprimento do plano, mas também para a tomada de medidas correctivas nos casos que se considerar necessário para dinamizar as iniciativas que estiverem a enfrentar desafios que ao nível técnico não estejam a encontrar soluções.

No final de cada ano, será feita a análise do plano anual, tendo como foco as actividades, objectivos e metas definidas para esse ano em particular e para o ano seguinte. Em 2024, ano em que termina o período de implementação desta estratégia, será feita a avaliação final do impacto da Estratégia Nacional de Segurança Cibernética e uma pesquisa, com objectivo de monitorar os níveis de maturidade no âmbito de segurança cibernética.

ii. Matriz de Monitoria

Deverá ser desenvolvida uma matriz de monitoria, com os principais indicadores, de impacto, desempenho e execução, a serem utilizados na avaliação da implementação das iniciativas propostas no âmbito desta PENSC, de modo a avaliar o impacto das iniciativas para a segurança do espaço cibernético.

iii. Instrumentos de Suporte

A monitoria e avaliação do PENSC, que envolve a recolha de dados fiáveis e relevantes, vai fazer parte integrante do Observatório Nacional de Segurança Cibernética (ONSC), baseada na plataforma *web*, que irá conter também os dados úteis e fiáveis das iniciativas do PENSC, para que sirva de suporte para a tomada de decisão política, estratégica e operacional.

O Observatório Nacional de Segurança Cibernética (ONSC) vai contar com uma infra-estrutura informática específica que irá permitir reunir, selecionar, analisar, armazenar e difundir informação relevante de carácter técnico científico, no âmbito da segurança do espaço cibernético nacional e interacção com outros observatórios a nível regional e internacional.

Os CSIRTs sectoriais, no âmbito das suas acções de prevenção e combate (resposta) aos abusos no espaço cibernético e ao cibercrime, vão alimentar o CSIRT Nacional que por sua vez vai alimentar o Observatório Nacional de Segurança Cibernética (ONSC).

iv. Divulgação

A informação resultante da monitoria e avaliação, como as tendências nos principais indicadores de impacto das iniciativas e projectos a nível sectorial e institucional, será comunicada através de diferentes canais e meios com vista a alcançar grupos alvo específicos. Tal incluirá pequenos resumos para os tomadores de decisões, apresentações em eventos nacionais e internacionais sobre a Sociedade de Informação, publicação de relatórios e artigos técnicos, publicações na *Internet*, e ainda *briefings* à imprensa e à comunicação social. os principais indicadores de impacto resultados do relatório serão resumidos e publicados no formato de *ranking* interno a nível sectorial e institucional, a ser definido com base nas boas práticas internacionais.

4. Financiamento

O custo total de implementação da PENSC é de 882 200,000.00Mt distribuídos pelas iniciativas e pelo período de execução, conforme a tabela em anexo, onde se indicam as prioridades, os responsáveis e os intervenientes. A principal fonte de financiamento é Orçamento do Estado, que poderá ser complementado por outros mecanismos de financiamento, em particular com o apoio e participação do sector privado, dos parceiros de cooperação e da academia.

Para além das iniciativas aqui listadas, as instituições do Estado são instadas a alocar 10% do seu orçamento do sector das TIC, em iniciativas e acções ligadas a área de segurança cibernética.

Tabela 3. *Custo da PENSC agregado por Pilar e Objectivo*

No.	Pilar	Objectivo específico	Valor (10^3) (MT)
1.	Liderança e Coordenação	Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética.	240,200.00
2	Protecção de Infra-estruturas Críticas de Informação	Proteger as ICI.	35,000.00
3.	Quadro Legal e Regulatório	Criar o quadro legal de segurança cibernética.	68,000.00
4.	Protecção de Activos de Informação	Proteger os Activos de Informação	134,000.00
5.	Desenvolvimento da capacidade de pesquisa e inovação	Desenvolver a capacidade técnico-operacional e de pesquisa e inovação em matéria de segurança cibernética.	345,000.00
6.	Cultura de Segurança Cibernética e de Consciencialização	Desenvolver programas e mecanismos de Consciencialização sobre os Riscos Associados ao uso do Espaço Cibernético.	60,000.00
Total			**882,200.00**

Conclusão

O país começou formalmente a sistematização dos esforços pela massificação do uso das TIC, quando o Governo aprovou a primeira Política de Informática, através da Resolução n.º 28/2000, de 12 de Dezembro. Desde então tornou-se imperiosa a adopção de medidas orientadoras que concorrem para resolução dos novos problemas associados com a revolução digital, que passam por políticas e estratégias que garantam (i) A regulação de funcionamento do ciberespaço; (ii) O desenvolvimento de capacidade individual, institucional e nacional em matéria de segurança cibernética; (iii) A protecção de infra-estruturas críticas e activos de informação; (iv) O estabelecimento de mecanismo de coordenação e colaboração institucional em matéria de segurança cibernética; e (v) A promoção de boas práticas no uso das TIC e do comportamento positivo no espaço cibernético.

Portanto, a PENSC constitui um importante passo para a dinamização dos esforços do desenvolvimento da economia e governação digital em Moçambique porque propõe princípios e mecanismos que orientam o país no abordar dos desafios da promoção de segurança cibernética das infra-estruturas críticas, das instituições do sector público, sector privado, da academia, da sociedade civil, e do cidadão. As tecnologias digitais emergentes tais como computação na nuvem, a *Internet* das Coisas (IoT), a Inteligência Artificial, BigData, mineração de dados, robótica entre outros, serão de forma holística e futurística, abordados no âmbito da segurança cibernética visto que estas tecnologias vão evoluir e prevalecer nos próximos tempos.

A visão de "uma nação com um espaço cibernético seguro, resiliente e uma sociedade consciencializada sobre os riscos no espaço cibernético" para o nosso país será materializada com a prossecução dos seis (6) objectivos estratégicos da Política de Segurança Cibernética e com o respeito dos Princípios Orientadores, que foram definidos de acordo com as condições socioculturais específicas da sociedade moçambicana.

A Política de Segurança Cibernética será materializada pela sua estratégia de implementação alinhada com os pilares e objectivos específicos desta política e define 25 iniciativas concretas a serem implementadas a curto, médio e longo prazo, e que concorrem para a materialização da visão e missão desta política.

A abordagem seguida na preparação e elaboração da PENSC foi democrática e inclusiva, o que assegurou que todos os actores sociais estivessem envolvidos e comprometidos com o sucesso desta, realçando-se a existência de um Conselho Nacional de Segurança Cibernética, que é uma estrutura de coordenação que envolve a representatividade e participação de todas as forças vivas da sociedade.

No entanto, para que efectivamente os objectivos da PENSC sejam alcançados, os Factores Críticos de Sucesso, nomeadamente a liderança, o capital humano e outros, incluindo o financiamento, terão que ser controlados e avaliados.

A PENSC é um importante instrumento da sociedade, em particular pelos agentes promotores do desenvolvimento nacional, e é uma das bandeiras e factores que concorrem para a avaliação da competitividade a nível regional, continental e global, e está agora disponível para ser usada por todos os interessados. Ela constitui, portanto, um instrumento orientador da governação do espaço cibernético em Moçambique, que se pretende seguro, inclusivo e sustentável, e que concorra para a realização de transacções electrónicas seguras a nível do comércio e governo electrónico, e para a promoção da economia digital, em prol do desenvolvimento económico e social do nosso país.

Glossário

Academia: Instituições vocacionadas para o ensino, a cultura e a ciência, nomeadamente as artísticas, literárias, científicas, físicas, filosóficas entre outras. O termo também pode se referir a qualquer associação de cientistas, literatos ou artistas.

Activo de Informação: Meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Ameaça cibernética: É um acto malicioso que visa destruir ou roubar dados ou a perturbação do funcionamento normal dos sistemas computacionais.

Ataque cibernético(*Hackers*): Actores mal-intencionados de danificar ou interromper o funcionamento normal de uma rede, sistema ou aplicativo de computador.

Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Ciberespaço: Espaço da comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores".

Confidencialidade: Assegurar que a informação é acessível somente à entidades devidamente autorizadas.

Cultura de cibersegurança: Alinhamento da cibersegurança com os objectivos da organização de criar um ambiente holístico de confiança e obtenção de resultados consistentes. Envolve a avaliação contínua do risco para criar um ambiente de TIC resiliente.

Crime Cibernético: Crimes que envolvem o uso de um computador e/ou rede de computadores. Pode ser num caso em que um computador é usado na prática de um crime ou em que o computador é o alvo do crime.

Cyberbullying: tipo de violência praticada contra alguém através da *internet* ou de outras tecnologias relacionadas, para intimidar e hostilizar uma pessoa (colega de escola, professores ou mesmo desconhecidos), difamando, insultando ou atacando covardemente.

Disponibilidade: Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Dark Web: Uma *Internet* obscura ou endereço sombrio refere-se a qualquer ou todos os servidores de rede inalcançáveis na *Internet*, por requererem *softwares*, configurações ou autorizações específicas para o acesso.

Deep web: (deepnet, *web* invisível, undernet, web obscura ou web oculta) corresponde à parte não indexada e surface web (ou *internet* superficial) é a parte indexada.

Grooming: aliciamento de menores através da *Internet*, com o intuito de se buscar benefícios sexuais, normalmente, ocorre por meio de fotos e vídeos conseguidos através das redes sociais, sites de jogos ou de animação ou mesmo de contacto físico e encontros presenciais esporádicos.

Infra-estruturas Críticas: instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, económico, político, internacional ou à segurança do Estado e da sociedade.

Infra-estruturas Críticas da Informação: subconjunto de activos de informação que afectam directamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

Integridade: É a garantia de que os dados permaneçam íntegros e sem qualquer alteração quando disponibilizados.

Malware: Programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

Maturidade da cibersegurança: Descrição de como uma organização garante a qualidade de sua implementação e gestão de cibersegurança e como as práticas são abordadas e sustentadas para criar valor.

Phishing: Tentativas de obtenção de informação pessoalmente identificável através de uma suplantação de identidade por parte de criminosos em contextos informáticos.

Ransomware: Tipo de *software* malicioso, que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido.

Segurança Cibernética: Protecção dos sistemas de TIC contra danos, roubo ou interrupção dos processos por estes executados. abrange a combinação de pessoas, processos e tecnologia.

Vulnerabilidade: Propriedade intrínseca de algo resultando em susceptibilidade a uma fonte de risco que pode levar a um evento com uma consequência. Conjunto de factores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma acção interna de segurança da informação.

Tecnologia Long Term Evolution: Também conhecida por 4G – Tecnologia-padrão de redes de celulares, que permite a velocidade da banda larga móvel chegar até 100Mbps.

Lista de Acrónimos

AFRICACERT		Equipas de resposta a Emergências computacionais para África.
AU-GFCE		Abreviação inglesa (Africa Union- Global Forun on Cyber Expertise)
CERT	-	Abreviação inglesa (*Computer Emergency Response Team*) - Equipas de Resposta a Emergências Computacionais
CFMP		Cenários Fiscais de Médio Prazo
CNDS	-	Conselho Nacional de Defesa e Segurança
CNSC		Conselho Nacional de Segurança Cibernética
CSIRT	-	Abreviação inglesa de Equipa de Resposta a Incidentes de Segurança de Computadores
CATI		Centro de Pesquisa e Análise de Tráfego de *Internet*
e-Mola		Carteira Móvel da Movitel
ENSC		Estratégia Nacional de Segurança Cibernética
FDS		Forças de Defesa e Segurança
GCI	-	Índice Global de Segurança Cibernética
IC	-	Infra-estrutura Crítica
ICI	-	Infra-estrutura Crítica de Informação
IDH		Índice do Desenvolvimento Humano
IEEE	-	Instituto de Engenheiros Electricistas e Electrónicos
IDI-ICT		Índice de Desenvolvimento das Tecnologias de Informação e Comunicação
INCM	-	Instituto Nacional das Comunicações de Moçambique
ISSM		Instituto de Supervisão de Seguros e Moçambique
INTIC	-	Instituto Nacional de Tecnologias de Informação e Comunicação
LFD	-	Laboratório de Forense Digital
Mkesh		Carteira Móvel da TMcel
Mpesa		Carteira Móvel da Vodacom
NU	-	Nações Unidas
OE		Objectivo Específico
ONSC		Observatório Nacional de Segurança Cibernética
PESI		Plano Estratégico para a Sociedade da Informação
PIB		Produto Interno Bruto
PENSC	-	Política e Estratégia Nacional de Segurança Cibernética
PNUD	-	Programa das Nações Unidas para o Desenvolvimento
SADC	-	Comunidade de Desenvolvimento da África Austral
SOC		Abreviação inglesa (National Security Operation Center) - Centro Nacional de Operações de Segurança Cibernética
STCNSC		Secretariado Técnico do Conselho Nacional de Segurança Cibernética
TI	-	Tecnologia da Informação
TIC	-	Tecnologias da Informação e Comunicação
TMCEL	-	Moçambique Telecom, SA
UA	-	União Africana
UIT	-	União Internacional de Telecomunicações

Preço — 140,00 MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.