República de Moçambique

Estratégia Nacional de Segurança Cibernética

Índice

Lista de Acrónimos

ENSC	-	Estratégia Nacional de Segurança Cibernética
PNSC		Política Nacional de Segurança Cibernética
CFMP		Cenários Fiscais de Médio Prazo
PESI		Plano Estratégico para a Sociedade da Informação
OE		Objectivo Específico
TIC		Tecnologias de Informação e Comunicação
GCI		Abreviação inglesa para Índice Global de Segurança Cibernética
UIT		União Internacional das Telecomunições
IDH		Índice de Desenvolvimento Humano
CNSC		Conselho Nacional de Segurança Cibernética
IDI-ICT		Índice de Desenvolvimento das Tecnologias de Informação e Comunicação
Mkesh, Mpesa e e-Mola		Carteiras móveis da TMcel, Vodacom e Movitel
CERT		Abreviação inglesa de Equipa de Resposta de emergências computacionais
ONSC		Observatório Nacional de Segurança Cibernética
SOC		Centro de Operações de Segurança Cibernética
CSIRT		Equipas de respostas a incidentes de eseguranca de computadores
ICI		Infraestrutura Crítica de Informação
STCNSC		Secretariado Técnico do Conselho Nacional de Segurança Cibernética
FDS		Forças de Defesa e Segurança

1 Sumário Executivo

A presente Estratégia Nacional de Segurança Cibernética (ENSC) tem em vista a materialização da Política Nacional de Segurança Cibernética (PNSC), tendo a sua execução alinhada com os Cenários Fiscais de Médio Prazo (CFMP), a implementar no horizonte de 2021-2024.

A ENSC está igualmente alinhada com os objectivos e acções inseridas no Plano Estratégico para a Sociedade da Informação (PESI), aprovado pela Resolução nº 52/2019, de 16 de Outubro, que vai até 2028 e contém algumas iniciativas de natureza cibernética, nomeadamente a Política Nacional de Segurança Cibernética, a Lei de Protecção de Dados Pessoais, a Lei de Transacções Electrónicas, programas de formação, capacitação, sensibilização e soluções tecnológicas que garantam transacções electrónicas seguras e privacidade no espaço cibernético.

Na PNSC estão definidos 6 pilares que constituem as principais áreas de actuação para o alcance da visão e da missão nela definidos, a saber:

I. Quadro de Governação da Segurança Cibernética;
II. Protecção de Infraestruturas Críticas de Informação (ICI);
III. Quadro Legal e Regulatório;
IV. Protecção de Activos de Informação;
V. Desenvolvimento de Capacidade, Pesquisa e Inovação; e
VI. Cultura de Segurança Cibernética e de Consciencialização.

A ENSC define um objectivo específico para cada pilar ou área de atuação, associando a cada um deles uma série de iniciativas, através das quais serão levadas a cabo várias acções que permitirão a materialização dos objectivos definidos, sendo estes os seguintes:

1. **Estabelecer mecanismo nacional de promoção de partilha, cooperação e coordenação em matéria de segurança cibernética**, onde se pretende criar organismos e plataformas de colaboração conjunta que permita uma boa governação no âmbito da segurança cibernética e evite a duplicação de esforços, que muitas vezes promove a incoerência das informações partilhadas pela multiplicidade das partes interessadas e relevantes nesta matéria, garantindo também a privacidade, confidencialidade, integridade de indivíduos, instituições, dados e sistemas;

2. **Melhorar a protecção da Infra-estrutura Crítica de Informação**, identificando em primeiro lugar as ICI existentes e as vulnerabilidades existentes de modo a criar mecanismos para a protecção destas contra ataques e incidentes, que possam causar danos ou disfunções das mesmas;

3. **Criar o quadro legal e técnico-operacional de segurança cibernética**, onde pretende-se desenvolver um quadro jurídico-administrativo integrado, capaz de harmonizar as práticas a nível nacional, regional e internacional, simplificar e efectivar o combate aos crimes cibernéticos proporcionando uma segurança jurídica no ciberespaço nacional;

4. **Melhorar a protecção dos Activos de Informação**, garantindo as liberdades individuais a privacidade e a integridade dos sistemas, instituições e pessoas, através da protecção da informação e das aplicações geradas, mantidas ou mesmo disponibilizadas através das plataformas tecnológicas, para que não sejam acedidas, destruídas ou modificadas de forma indevida;

5. **Desenvolver a capacidade técnico-operacional, de pesquisa e inovação em matérias de segurança cibernética**, criando capacidades técnicas e operacionais a nível nacional, capazes de apresentar soluções sistemáticas e apropriadas, para todos os aspectos relacionados com a mitigação dos crimes cibernéticos, a criação de mecanismos de detecção e prevenção dos crimes, assim como promover e fortalecer, o potencial local de investigação e de desenvolvimento de processos, tecnologias e soluções inovadoras e de vanguarda para a segurança cibernética;

6. **Criar uma cultura nacional de segurança cibernética**, de modo a tornar o cidadão cada vez mais consciente sobre as ameaças e riscos a que está sujeito ao utilizar os meios tecnológicos e os espaços cibernéticos para aceder ou disponibilizar serviços ou informação, tendo maior atenção às camadas mais vulneráveis como crianças, deficientes e mulheres.

As iniciativas e os objectivos da ENSC não só são consentâneas com o estágio actual do desenvolvimento das TIC em Moçambique, mas também contribuem para melhorar significativamente a sua posição no Índice Global de Segurança Cibernética (GCI), pois preveem a implementação de normas, padrões, condutas e procedimentos baseados em critérios usados pela União Internacional das Telecomunições (UIT) na avaliação de países. Para a elaboração tanto da PNSC assim como da ENSC foram observadas as orientações emanadas na convenção da União Africana sobre segurança cibernética e protecção de dados pessoais.

A ENSC também estabelece um modelo de governação inspirado no modelo sugerido pela Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais (Resolução Nº 5/2019, de 20 de Junho), onde a liderança do que está preconizado é ao mais alto nível e privilegia a partilha de responsabilidades, a coordenação transversal e uma ampla auscultação dos parceiros sociais, através da criação do Conselho Nacional de Segurança Cibernética (CNSC), um órgão dirigido pelo Presidente da República.

A estratégia prevê igualmente a criação de equipes técnicas que, através de várias medidas e plataformas que serão estabelecidas, permitirão que o cidadão e as instituições, tenham acesso ao aconselhamento e à informação sobre os mecanismos necessários para a sua protecção no espaço cibernético. Estas plataformas servirão de igual modo, para promover uma cultura e uma mentalidade, dos aspectos de segurança cibernética a ter em conta,

quando tanto as instituições ou as pessoas se expõem usando as TIC, para prover ou aceder a serviços ou informação. Especial atenção será dada às crianças e aos grupos de cidadãos com vulnerabilidade de qualquer tipo, na criação de uma cultura e dum ambiente seguro, para o uso do espaço cibernético.

Para a monitoria e avaliação das acções estabelecidas na ENSC, prevê-se que sejam estabelecidos planos anuais, contendo as iniciativas e acções eleitas para implementação nesse período, estabelecendo igualmente os indicadores de desempenho para cada uma das iniciativas de modo a facilitar a avaliação do seu cumprimento, estando esta tarefa sobre a responsabilidade do CNSC, órgão máximo de governação da segurança cibernética no país.

2 Contextualização

O índice de desenvolvimento de qualquer nação está intrinsecamente ligado à adopção das novas tecnologias de informação e comunicação devido à sua transversalidade e à sua capacidade de mitigar os taques cibernéticos associados.

Moçambique é um país detentor de enormes reservas de gás natural na sua plataforma marítima continental e espera-se que a médio prazo se torne num dos maiores exportadores de hidrocarbonetos, capitalizando os ganhos na recuperação do desenvolvimento socioeconómico, em benefício das suas populações. Apesar das várias riquezas naturais existentes no país e dos vários esforços que têm sido levados a cabo pelo governo para melhorar a posição de Moçambique nos vários índices de desenvolvimento apresentados, tal como no Índice de Desenvolvimento Humano (IDH), em 2019, Moçambique situou-se na posição 180, com 0.446 valores, entre os 188 avaliados.

A posição alcançada por Moçambique no IDH de 2019, revela um crescimento moderado registado nas últimas décadas. Este resultado foi alcançado, graças ao esforço em investimento que o país tem levado a cabo, nas áreas de educação, saúde, emprego e infraestruturas sociais e económicas. Mas, porque o país parte de uma base bastante precária, que ainda não permitiu induzir melhorias significativas na qualidade de vida da população, continua, entre os últimos 10 lugares do *ranking* mundial.

De entre as várias melhorias que o governo tem estado a empreender no país, encontra-se igualmente a elevação do nível de eficiência e eficácia, a redução da burocracia e da corrupção no país e a melhoria na prestação dos serviços públicos oferecidos. Para tal, tem-se apostado na digitalização dos serviços públicos oferecidos, ajudando deste modo, a melhorar os resultados nos índices acima referidos, através das profundas transformações que o governo tem estado a empreender, nos processos envolvidos na prestação de serviços, assim como na forma como lida com o cidadão e com os bens públicos. Estas transformações, se têm refletido paulatinamente em substanciais melhorias na governação e na vida das populações e consequentemente em melhorias económicas, sociais e culturais.

No Índice de Desenvolvimento das Tecnologias de Informação e Comunicação (IDI - ICT Development índex) de 2016[1], que dá a indicação da posição de cada país em relação ao uso

[1] http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

das novas tecnologias, Moçambique teve a posição 123ª., num *ranking* de 139 países avaliados, subindo sete posições, comparativamente ao ano anterior em que se encontrava na 129ª. , posição do *ranking* de 2015. Esta subida de sete posições, foi resultado dos grandes esforços que o Governo tinha estado a levar a cabo, investindo em infraestruturas que permitiram o acesso aos serviços e à informação, investindo no desenvolvimento de capacidades e na disseminação do uso das TIC. Observe que o Relatório de Tecnologia da Informação Global 2016 é a última edição da série. Não houve actualizações disponíveis.

Um dos grandes ganhos do país, provenientes dos esforços com a digitalização é a introdução de carteiras móveis, tais como Mkesh, Mpesa e e-Mola que permitem fazer pagamentos sem que o cidadão tenha que carregar consigo o valor monetário físico, facilitando deste modo as transacções electrónicas entre pessoas e até empresas e a vida da maioria da população moçambicana, sobretudo a que reside nas zonas rurais. Através destas carteiras moveis é igualmente possível, fazer pagamento de serviços básicos tais como água, energia, televisão e a compra de crédito para a comunicação.

A introdução dos serviços de carteira móvel, e-banca, serviços de governo electrónico, formação e educação a distancia com recurso as plataformas tecnológicas assim como de outros serviços que facilitam a vida do cidadão, foi facilmente aderida, apesar do conhecimento sobre os perigos e precauções que devem ser tomadas ser ainda muito baixo. À medida que o uso destas tecnologias se vai ampliando, aumenta também a exposição de quem as usa e os crimes de burla, roubo de identidade, ataques phishing, ransomware,

negação de serviços, assim como muitos outros crimes que acontecem no espaço cibernético.

Estando ciente dos prejuízos de vária ordem que advêm, das actividades criminosas nesta área e do impacto destes no crescimento socioeconómico do país, o Governo pretende reforçar a sua capacidade de prevenir, detectar e combater este tipo de crimes através das várias medidas e iniciativas que são apresentadas nesta estratégia.

3 Missão e Visão

A missão e visão aqui apresentadas foram definidas no âmbito da Política Nacional de Segurança Cibernética.

3.1 Missão

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

3.2 Visão

Uma nação com um espaço cibernético seguro, resiliente e uma sociedade consciencializada.

4 Objectivo Geral

Assegurar a protecção de Activos de Informação e suas Infra-estruturas Críticas no

espaço cibernético.

4.1 Objectivos Específicos

Para atender à visão e missão propostas, na Política Nacional de Segurança Cibernética, bem como ao objectivo geral aqui traçado e as necessidades em segurança cibernética decorrentes do estágio de maturidade do ecossistema digital do país, foram definidos 6 objectivos específicos, que visam orientar as acções estratégicas que são essenciais e necessárias para que o país possa prevenir e detectar as tentativas de ataques cibernéticos bem como mitigar e resolver os problemas advindos das vulnerabilidades no espaço cibernético.

Os objectivos específicos abaixo definidos, servem de diretrizes para que o setor público e privado assim como a sociedade civil usufruam de um espaço cibernético resiliente, confiável, inclusivo e seguro:

1. Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética;
2. Melhorar a protecção da infraestrutura crítica de informação (ICI);
3. Criar o quadro legal e técnico-operacional de segurança cibernética;
4. Melhorar a protecção dos Activos de Informação, e
5. Desenvolver a capacidade técnica de pesquisa e inovação em matéria de segurança cibernética;
6. Criar programas e mecanismos de consciencialização sobre os Riscos associados ao uso de espaços cibernéticos.

5 Iniciativas a Desenvolver

Em cada pilar ou área de actuação foi definido um objectivo específico, associando a este, uma série de iniciativas a serem levadas a cabo para a sua materialização e que estão descritas a seguir.

5.1 Objectivo Específico 1 (OE1): Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética

Num espaço cibernético não existem fronteiras e as ameaças que ocorrem são sofisticadas e complexas, requerendo assim, a criação de órgãos e a institucionalização destes, de modo a garantir a promoção, partilha, coordenação e colaboração das acções a serem levadas a cabo no âmbito da segurança cibernética. Estes órgãos, deverão igualmente garantir as liberdades individuais, a integridade das instituições e das pessoas, que usam e disponibilizam serviços e informação no espaço cibernético nacional. Assim, serão desenvolvidas as seguintes iniciativas:

- ✓ Criar e institucionalizar o Conselho Nacional de Segurança Cibernética (CNSC);
- ✓ Criar e institucionalizar a Equipa de Resposta a Incidentes Informáticos a Nível Nacional (CERT Nacional – National Computer Emergency Response Team);

- ✓ Criar Equipas de Resposta a Incidentes de Informáticos (CSIRT - Computer Security Incident Responce Team), sectorias e nas instituições com ICI e Activos de Informação;
- ✓ Criar e institucionalizar o Centro de Operações de Segurança Cibernética a nível Nacional (SOC Nacional – National Security Operation Center); e
- ✓ Desenvolver o Observatório Nacional de Segurança Cibernética (ONSC).

5.2 Objectivo Específico 2 (OE2): Melhorar a Protecção da Infraestrutura Crítica de Informação

É primordial que o Governo identifique e proteja as ICI, sobretudo porque os ataques e incidentes cibernéticos poderão causar danos e disrupção do funcionamento da economia nacional, incluindo a integridade, vida e saúde das pessoas.

Os danos podem incluir o enfraquecimento da segurança territorial e da estabilidade do Estado, à reputação dos indivíduos, das instituições públicas e privadas, sendo imperativo que Moçambique priorize a segurança cibernética das suas ICI, tornando-as seguras e resilientes.

A protecção das ICI e outras infraestruturas de informação de Moçambique é uma responsabilidade partilhada de todos os utilizadores de TICs e requer a colaboração das partes interessadas, nomeadamente os sectores público e privado e a sociedade civil que possuam e/ou explorem infraestruturas de informação. Devendo todos trabalhar em conjunto na avaliação dos níveis de segurança cibernética e nas vulnerabilidades das infraestruturas de informação de Moçambique, implementando medidas e/ou acções que atenuem ou resolvam as ameaças e os riscos cibernéticos actuais e futuros, implementando as seguintes iniciativas:

- ✓ Mapear as ICI de Moçambique, identificando os riscos e vulnerabilidades existentes e os incidentes de segurança cibernética que nelas ocorrem;
- ✓ Estabelecer o modelo de colaboração entre as Equipes de Resposta a Incidentes de Segurança Cibernética a Nível Nacional para a protecção das ICI do pais; e
- ✓ Estabelecer os procedimentos para a auditoria das ICI.

5.3 Objectivo Específico 3 (OE3): Criar um quadro legal de segurança cibernética

Espera-se que todos os utilizadores de TIC em Moçambique tomem medidas para garantir a sua segurança cibernética e combater os crimes que ocorrem nesse espaço. Para tal, é necessário que um ambiente propício seja criado e que facilite os esforços dos utilizadores das TIC na garantia da sua segurança cibernética e na luta contra a criminalidade cibernética. Neste contexto, o Governo deve criar um quadro legal, regulatório e técnico operacional de segurança cibernética que garanta a criação de mecanismos de prevenção, detecção e repressão de actividades criminosas no espaço cibernético.

As leis criadas deverão igualmente, ser aplicadas em situações de insegurança cibernética e orientar os utilizadores das TIC na adopção de práticas consistentes de segurança cibernética.

O quadro legal de segurança cibernética desejado será criado, através da implementação das iniciativas abaixo assim como de outras que se mostrarem necessárias:

- ✓ Rever e harmonizar o quadro legal existente, incluindo nele matérias referentes a crimes de segurança cibernética;
- ✓ Reforçar o quadro legal sobre Segurança Cibernética;
- ✓ Promover e Divulgar o quadro legal sobre segurança cibernética;
- ✓ Ratificar convenções internacionais sobre segurança cibernética; e
- ✓ Assinar acordos de cooperação judiciária em matérias de cibercriminalidade.

5.4 Objectivo específico 4 (OE4): Melhorar a protecção dos Activos de Informação,

Os activos de informação constituem um importante recurso para o desenvolvimento, segurança e defesa das nações, e qualquer impedimento ao seu acesso ou a sua destruição ou usurpação, podem pôr em causa a confiança dos cidadãos no Estado, em lidar com os seus interesses particulares, com a causa pública e até comprometer a soberania do país. Assim para que as instituições e pessoas possam disponibilizar ou usar serviços e informação no espaço cibernético sem o temor de pôr em causa as suas liberdades individuais e a sua integridade, serão desenvolvidas as seguintes iniciativas:

- ✓ Estabelecer sistemas de mitigação e alerta dos incidentes cibernéticos;
- ✓ Criar mecanismos de filtragem e remoção de conteúdos ilegais; e
- ✓ Estabelecer programas de simulação dos incidentes de segurança cibernética.

5.5 Objectivo Específico 5 (OE5): Desenvolver a capacidade técnico-operacional e de pesquisa e inovação em matéria de segurança cibernética

Os rápidos avanços na área de tecnologias de informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas actividades, inclusive a oferta de serviços por parte do Governo e das empresas privadas, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade. Ciente desta situação o Governo reconhece que o desenvolvimento da capacidade técnica de modo a profissionalizá-la em matérias de segurança cibernética em todo o país é crucial, para criar as habilidades necessárias e adequadas de prevenir, monitorar, detectar e dirimir ameaças e incidentes cibernéticos que possam ocorrer no nosso espaço cibernético. Assim serão desenvolvidas as seguintes iniciativas, que concorrem para a capacitação e desenvolvimento da capacidade técnico-operacional e de pesquisa e inovação, no país:

- ✓ Criar capacidade técnico-operacional de defesa e resposta a incidentes de segurança cibernética no país;
- ✓ Desenvolver programas de capacitação e de criação de habilidades técnicas e operacionais em segurança cibernética;
- ✓ Promover o desenvolvimento de pesquisas que busquem soluções inovadoras na área de segurança Cibernética; e

- ✓ Estabelecer parcerias de colaboração técnica a nível local, regional e internacional na prevenção e no combate ao crime cibernético.

5.6 Objectivo especifico 6 (OE6): Criar programas e mecanismos de Consciencialização Sobre os Riscos Associados ao Uso de Espaços Cibernéticos

A maioria dos incidentes de segurança cibernética podem ser prevenidos ou atenuados quando todos os utilizadores das TIC estiverem cientes e compreenderem as ameaças e tendências da segurança cibernética. Para tal, é importante que os indivíduos e as instituições tomem medidas de segurança no espaço cibernético implementando boas práticas no uso da Internet. Além disso, o Governo entende que é responsável pela protecção das crianças e de outros grupos vulneráveis, incluindo a sua protecção na Internet.

As crianças e outros usuários vulneráveis são geralmente vítimas de *cyberbullying*, solicitação sexual e *grooming* (aliciamento), pornografia infantil e outros conteúdos nocivos. Assim para minimizar a exposição destes, serão realizadas as seguintes acções:

- ✓ Realizar um inquérito nacional de avaliação do nível de consciencialização dos Sectores público e privado e da sociedade civil em segurança cibernética;
- ✓ Realizar campanhas de consciencialização sobre segurança cibernética com especial enfoque na protecção da criança e de outros grupos vulneráveis; e
- ✓ Definir fóruns de elevação do nível de maturidade dos Sectores público e privado e sociedade civil em segurança cibernética.

6 Alinhamento dos Pilares, Objectivos Específicos e Iniciativas a Implementar

Pilares	Objectivos Específicos		Iniciativas a Implementar	
Quadro de Governação da Segurança Cibernética	OE1	Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética	I01	Criar e institucionalizar o Conselho Nacional de Segurança Cibernética (CNSC).
			I02	Criar e institucionalizar a Equipa de Resposta a Incidentes Informáticos a Nível Nacional (CERT Nacional).
			I03	Criar Equipas de Resposta a Incidentes de Informáticos (CSIRT), Sectorias nas instituições com ICI e activos de Informação.
			I04	Criar e institucionalizar o Centro de Operações de Segurança Cibernética a nível Nacional (SOC Nacional)
			I05	Desenvolver o Observatório Nacional de Segurança Cibernética (ONSC).
Protecção de Infraestrut	OE2		I06	Mapear as ICI de Moçambique, identificando os riscos e vulnerabilidades existentes e os incidentes de segurança cibernética que nelas ocorrem

Pilares	Objectivos Específicos		Iniciativas a Implementar	
		Melhorar a protecção das ICI	I07	Estabelecer o modelo de colaboração entre as Equipes de Resposta a Incidentes de Segurança Cibernética a Nível Nacional para a protecção das ICI do país
			I08	Estabelecer os procedimentos para a auditoria das ICI
Quadro Legal e Regulatório	OE3	Criar o quadro legal de segurança cibernética	I09	Rever e harmonizar o quadro legal existente
			I10	Reforçar o quadro legal sobre Segurança Cibernética
			I11	Ratificar convenções internacionais sobre segurança cibernética
			I12	Assinar acordos de cooperação judiciária em matérias de cibercriminalidade
			I13	Promover e Divulgar o quadro legal sobre segurança cibernética
Protecção de Activos de Informação	OE4	Melhorar a Proteçcão de Activos de Informação	I14	Estabelecer sistemas de alerta dos incidentes cibernéticos
			I15	Criar mecanismos de filtragem e remoção de conteúdos ilegais
			I16	Estabelecer programas de simulação dos incidentes de segurança cibernética
Desenvolvimento de Capacidade, Pesquisa e Inovação	OE5	Desenvolver a capacidade técnico-operacional e de pesquisa e inovação em matéria de segurança cibernética	I17	Criar a capacidade técnico-operacional de resposta a segurança cibernética no país
			I18	Promover o desenvolvimento de pesquisas que busquem soluções inovadoras na área de segurança Cibernética
			I19	Desenvolver programas de capacitação e de criação de habilidades técnicas e operacionais em segurança cibernética
			I20	Estabelecer parcerias de colaboração técnica a nível local, regional e internacional na prevenção e no combate ao crime cibernético
Cultura de Segurança Cibernética e de Consciencialização	OE6	Criar programas e mecanismos de Consciencialização Sobre os Riscos Associados ao Uso de nos Espaços Cibernéticos	I21	Realizar um inquérito nacional de avaliação do nível de consciencialização dos Sectores público e privado e da sociedade civil em segurança cibernética
			I22	Desenvolver programas de consciencialização sobre segurança cibernética com especial enfoque na protecção da criança e de outros grupos vulneráveis
			I23	Realizar campanhas de consciencialização sobre segurança cibernética com especial enfoque na protecção da criança e de outros grupos vulneráveis

7 Descrição das Acções a Serem Implementadas em Cada Iniciativa

A tabela abaixo, apresenta a descrição das iniciativas definidas como forma de materializar os objectivos específicos traçados no âmbito desta ENSC, assim como as acções que serão executadas em cada uma delas e os resultados esperados. A implementação destas iniciativas estará sujeita a aprovação dum cronograma pelo CNSC, depois de definidas as prioridades para a execução das mesmas de acordo com os recursos humanos, materiais e financeiros disponíveis.

OE1- Estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética	
Código do Projecto: OE1-I01	
Iniciativa	Criar e institucionalizar o Conselho Nacional de Segurança Cibernética (CNSC)
Descrição	O CNSC é o órgão de governação da segurança cibernética do país, sendo a sua criação e institucionalização imprescindível para a implementação desta estratégia e através desta iniciativa, serão levados a cabo todos os processos legais necessários para criação, institucionalização e entrada em funcionamento do CNSC.
Entregáveis	1. Decreto de criação do CNSC aprovado e publicado; 2. Estatutos para o início de actividades do CNCS aprovados; e 3. CNSC oficialmente estabelecido e as condições para a entrada em funcionamento deste órgão, igualmente estabelecidas
Código do Projecto: OE1-I02	
Iniciativa	Criar e institucionalizar a Equipa de Resposta a Incidentes Informáticos a Nível Nacional (CERT Nacional – National Computer Emergency Response Team);
Descrição	O CERT Nacional, será um órgão de coordenação nacional das equipes de resposta a incidentes cibernéticos (CISIRT), que deve ser estabelecido e institucionalizado. Devendo este ser constituído por um grupo de pessoas especializadas nesta matéria, tendo a responsabilidade de proteger o país contra ameaças de crimes cibernéticos assim como dar respostas adequadas aos incidentes que ocorrerem no nosso espaço cibernético nacional. Assim para o seu estabelecimento, institucionalização e entrada em funcionamento, serão levados a cabo todos os tramites legais necessários.

Entregáveis	1. Diploma Ministerial de criação do CERT Nacional aprovado e publicado; 2. Estatutos para o início de actividades do CERT Nacional aprovados; e 3. CERT Nacional oficialmente estabelecido e apto a exercer o seu papel
Código do Projecto: OE1-I03	
Iniciativa	Criar Equipas de Resposta a Incidentes de Informáticos (CSIRT - Computer Security Incident Responce Team), nas instituições com ICI e Activos de Informação
Descrição	Identificação dos técnicos nas instituições com ICI e activos de informação para os quais maior atenção deverá ser dada para a sua protecção, que poderão constituir a CSIRT desse sector e que irá trabalhar em coordenação com o CERT Nacional.
Entregáveis	1. CSIRT sectoriais formalmente estabelecidas; e 2. Definido o modelo de colaboração e coordenação entre o CERT Nacional e as CSIRT sectoriais.
Código do Projecto: OE1-I04	
Iniciativa	Criar e institucionalizar o Centro de Operações de Segurança Cibernética a nível Nacional (SOC Nacional – National Security Operation Center)
Descrição	O Centro de Operações de Segurança Cibernética é uma plataforma de prestação de serviços com capacidade de observar e identificar eventos de segurança cibernética, recolher informação sobre os mesmos, analisá-la e reagir caso seja necessário. Esta plataforma deve igualmente manter o registo de todos os eventos occoridos e das acções levadas a cabo em cada um deles. Para o seu estabelecimento será necessário: ✓ Identificar o local onde o mesmo será instalado de acordo com as condições existentes; e ✓ Estabelecer o centro legalmente e dotá-lo de recursos materiais, humanos e financeiros essenciais para o seu funcionamento.
Entregáveis	1. SOC Nacional formalmente estabelecido e em funcionamento; e 2. Modelo de colaboração entre este centro e o CERT igualmente estabelecido
Código do Projecto: OE1-I05	

Iniciativa	Desenvolver o Observatório Nacional de Segurança Cibernética (ONSC)
Descrição	Desenhar, criar e estabelecer os mecanismos para a atualização constante de uma plataforma *on-line* (Observatório Nacional de Segurança Cibernética), com informações relacionadas às ICI, aos activos de informação, às ameaças, vulnerabilidades e incidentes cibernéticos que neles ocorrem e definir os níveis de acessibilidade desta informação pelas instituições públicas, privadas e sociedade civil
Entregáveis	1. Observatório Nacional de Segurança Cibernética disponível; e 2. Mecanismos para a atualização do ONSC estabelecidos
OE2- Melhorar a Protecção das ICI	
Código do Projecto: OE2-I06	
Iniciativa	Mapear as ICI de Moçambique, identificando os riscos e vulnerabilidades existentes e os incidentes de segurança cibernética que nelas ocorrem
Descrição	Identificar as ICI existentes e fazer o mapeamento destas de acordo com o tipo e dimensão e outras características relevantes a definir e criar um registo das mesmas, incluindo nele os riscos e vulnerabilidades existentes que propiciam a existência de incidentes de segurança cibernética. De entre as várias acções a serem levadas a cabo destacam-se as seguintes: ✓ Definição de critérios para eleição das infraestruturas criticas. ✓ Definição dos dados a incluir no mapeamento das ICI e sua disposição; ✓ Identificação das ICI e seu mapeamento; ✓ Criar um mecanismo de monitoria, avaliação e testagem regular das ICI de modo a emitir alertas ao detectar erros, vulnerabilidades e intrusões e sugerir medidas de prevenção e mitigação dos incidentes; ✓ Estabelecer as directrizes necessárias que promovam a avaliação e gestão destes nas ICI.
Entregáveis	4. Documento contendo critérios de avaliação e de identificação de ICI e sua eleição; 5. Formulário para o registo de informação sobre as ICI e dos dados a serem recolhidos; e 6. Base de dados contendo informação relevante das ICI eleitas, incluindo o registo de incidentes, vulnerabilidades, intrusões e gestão das ICIs.

Código do Projecto: OE2-I07	
Iniciativa	Estabelecer o modelo de colaboração entre as Equipes de Resposta a Incidentes de Segurança Cibernética a Nível Nacional para a protecção das ICI do país
Descrição	Estabelecer políticas ou regulamentos sobre procedimentos de segurança cibernética para as ICI, que devem ser revistas continuamente e que permitam de entre outros aspectos definir: ✓ O controle do acesso às ICI; ✓ O plano de continuidade do negócio; ✓ As acções a desenvolver para minimizar os riscos de ataques e lidar com as ameaças à segurança do espaço cibernético nacional ✓ Sistemas de monitoria, avaliação e testagem regular das ICI de modo a emitir alertas ao detectar erros, vulnerabilidades e intrusões e sugerir medidas de prevenção e mitigação dos incidentes; ✓ Sistemas nas organizações com infraestruturas críticas que notifiquem o CERT Nacional dos incidentes cibernéticos; e ✓ Os requisitos específicos de segurança cibernética a serem usados pelos membros do governo e organizações públicas, equipamentos finais conectados a um terminal de alguma rede ou a algum sistema de comunicação.
Entregáveis	1. Regulamentos sobre procedimentos de segurança das ICIs estabelecidos; 2. Mecanismo de monitoria, avaliação e testagem regular das ICIs estabelecidos; 3. Mecanismos de notificação de incidentes cibernéticos nas ICTs estabelecidos; e 4. Procedimentos para a protecção das ICIs contra ameaças e ataques cibernéticos estabelecidos
Código do Projecto: OE2-I08	
Iniciativa	Estabelecer os procedimentos para a auditoria das ICI
Descrição	Uma vez criados os procedimentos para a protecção das ICI, é necessário que se verifique se os mesmos estão sendo aplicados por cada provedor de ICI, tornando-se assim necessário estabelecer um programa de auditorias regulares nas ICI de modo a educar os provedores de ICI e sancionar em casos de recorrência das anomalias registadas.
Entregáveis	1. Programa de auditorias às ICIs estabelecido;

	2. Modelo de auditorias a serem realizadas e resultados esperados definidos; e 3. Elaborados os procedimentos para as auditorias a realizar.
OE3- Criar um quadro legal de segurança cibernética	
Código do Projecto: OE3-I09	
Iniciativa	Rever e harmonizar o quadro legal existe, incluindo nele matérias referentes a crimes de segurança cibernética
Descrição	Rever a legislação penal e outros instrumentos legais vigentes no país de modo a incluir os aspectos relacionados com os crimes cibernéticos e a violação do espaço cibernético nacional e criar um registo dos aspectos revistos em cada instrumento legal.
Entregáveis	1. Instrumentos legais vigentes revistos e ajustados para acomodar os crimes cibernéticos; 2. Registo da legislação revista e actualizada e dos aspectos nela incorporados;
Código do Projecto: OE3-I10	
Iniciativa	Reforçar o quadro legal sobre Segurança Cibernética;
Descrição	Desenvolver os instrumentos legais e regulatórios para a protecção das ICI, protecção dos Activos de Informação, protecção dos utilizadores e do espaço cibernético nacional, incluindo os planos de conformidade que facilitem a aplicação destes.
Entregáveis	1. Relação cronológica de instrumentos legais a serem estabelecidos de acordo com as prioridades; 2. Instrumentos legais criados e aprovados;
Código do Projecto: OE3-I11	
Iniciativa	Ratificar convenções internacionais sobre segurança cibernética
Descrição	Identificar as convenções e os tratados que Moçambique pode ratificar na área de segurança cibernética que permitam resolver ou remir os possíveis conflitos que possam existir resultantes de crimes cibernéticos praticados dentro ou fora do país.
Entregáveis	1. Registo de convenções e tratados importantes para a resolução de conflitos; e 2. Ratificação das convenções e tratados identificados.

Código do Projecto: OE3-I12	
Iniciativa	Assinar acordos de cooperação judiciária em matérias de cibercriminalidade
Descrição	Identificar as situações para as quais o país necessita de celebrar acordos de cooperação judiciária para prevenir e combater o crime cibernético e proceder com a assinatura dos mesmos
Entregável	1. Tipo de acordos a assinar e os aspectos a serem cobertos nos mesmos identificados; e 2. Acordos assinados de acordo com as necessidades identificadas.
Código do Projecto: OE2-I13	
Iniciativa	Promoção e Divulgação do quadro legal sobre segurança cibernética
Descrição	Desenvolver um plano de promoção e divulgação da legislação sobre segurança cibernética para que o público tenha domínio de modo a torná-la pública.
Entregável	Plano de promoção e divulgação estabelecido, com indicação do tipo de actividades periódicas a realizar.
OE4- Melhorar a Protecção de Activos de Informação	
Código do Projecto: OE4-I14	
Iniciativa	Estabelecer sistemas de mitigação e alerta dos incidentes cibernéticos
Descrição	Uma das melhores formas de prevenção dos ataques cibernéticos é o tipo de sistemas de alerta que devem ser estabelecidos em cada activo de informação, de acordo com o seu tipo.
Entregáveis	Sistemas de mitigação e alerta identificados e funcionais
Código do Projecto: OE4-I15	
Iniciativa	Criar mecanismos filtragem e remoção de conteúdos ilegais
Descrição	Estabelecer os mecanismos necessários para filtrar e remover conteúdos legais de modo proteger a segurança nacional, preservar os valores culturais e religiosos e proteger os direitos de propriedade intelectual e a integridade das instituições e pessoas
Entregáveis	Mecanismos de filtragem e remoção de conteúdos ilegais estabelecidos

Código do Projecto: OE4-I16	
Iniciativa	Estabelecer programas de simulação dos incidentes de segurança cibernética
Descrição	Desenvolver programas de simulação de incidentes de segurança cibernética para testar os sistemas de protecção estabelecidos, nos activos de informação, contra os ataques cibernéticos, para avaliar a eficácia destes e assegurar a redução do risco de fuga de informações assim como a confidencialidade, integridade e disponibilidade dos dados, informação e sistemas de disponibilização de serviços
Entregáveis	1. Sistemas de simulação de incidentes instalados; e 2. Existência duma base de dados com informação sobre os testes efectuados em cada activo de informação e os seus resultados.
OE5- Desenvolver a capacidade técnico-operacional, de pesquisa e de inovação em matéria de segurança cibernética	
Código do Projecto: OE5-I17	
Iniciativa	Criar capacidade técnico-operacional de resposta a incidentes de seguranca cibernética
Descrição	Desenvolver programas de criação de capacidades técnico-operacionais, que possam solucionar todo tipo de incidentes cibernéticos que ocorram no país, devendo para tal: ✓ Identificar o arsenal de técnicos com conhecimentos em matérias de segurança cibernética na administração pública e os requisitos para a sua profissionalização; ✓ Criar programas de capacitação que respondam às necessidades de técnicos para responder aos incidentes cibernéticos que ocorrem; ✓ Rever e actualizar o currículo de educação formal, primário, secundário, médio e superior por forma a incluir matérias de segurança cibernética e permitir a profissionalização de quadros nacionais em segurança cibernética; e ✓ Criar carreiras de profissionais especializados na área de segurança cibernética, na administração pública.
Entregáveis	1. Identificado o arsenal de técnicos na função pública; 2. Criados programas de capacitação e garantida a existência de técnicos que possam dar vazão aos incidentes cibernéticos; 3. Revisto o currículo de ensino primário, secundário, médio e superior e inseridos os aspectos sobre segurança cibernética; e 4. Criada a carreira de profissionais de segurança cibernética na administração pública.

Código do Projecto: OE5-I18	
Iniciativa	Promover o desenvolvimento de pesquisas que busquem soluções inovadoras na área de segurança Cibernética
Descrição	Rever a agenda nacional de investigação para promover e incentivar a criação de centros de desenvolvimento de pesquisas em segurança cibernética e promover a realização de competições de soluções inovadoras resultantes das pesquisas realizadas. Criar ainda, um programa de incentivos para as empresas nacionais que fornecerem soluções inovadoras para a segurança cibernética, resultantes das actividades de pesquisa que desenvolvem.
Entregáveis	1. Revista a agenda nacional de investigação e elaboradas as directrizes para a criação de centros de pesquisa; 2. Identificados os modelos para a realização de competições de soluções inovadoras em segurança cibernética; e 3. Estabelecidos os critérios e mecanismos de estímulo para as empresas nacionais que apresentem soluções inovadoras resultantes de actividades de pesquisa desenvolvidas.
Código do Projecto: OE5-I19	
Iniciativa	Desenvolver programas de capacitação e de criação de habilidades técnicas e operacionais em segurança cibernética
Descrição	Desenvolver programas de capacitação e de criação de habilidades técnicas e operacionais para as várias instituições da administração pública e que estejam de acordo com o papel que cada uma destas instituições irá desempenhar para a materialização desta estratégia. Os programas devem garantir que sejam asseguradas as capacidades e habilidades para: ✓ Lidar eficazmente com incidentes cibernéticos cada vez mais sofisticados; ✓ Interpretar a legislação sobre segurança cibernética e garantir a sua aplicação; e ✓ Prevenir, investigar, produzir provas e detectar os ataques cibernéticos e sancionar os crimes. Deve-se incluir ainda programas para a formação de dirigentes da administração pública em segurança cibernética.
Entregáveis	Desenvolvidos os programas de capacitação e de criação de habilidades técnicas e operacionais em segurança cibernética de acordo com o público alvo
Código do Projecto: OE5-I20	

Iniciativa	Estabelecer parcerias de colaboração técnica a nível local, regional e internacional na prevenção e no combate ao crime cibernético
Descrição	Estabelecer parcerias que permitam: ✓ Uma colaboração de técnicos a nível local, regional e internacional, para a troca de experiências e a elevação da capacidade nacional na prevenção e combate ao crime cibernético; ✓ O estabelecimento de centros de excelência para a formação e desenvolvimento de pesquisas em segurança cibernética; e ✓ Estimular o surgimento de *startups* na área de segurança cibernética e incentivar o desenvolvimento de competências e de soluções em criptografia
Entregáveis	1. Parcerias estabelecidas para: a) A colaboração e intercâmbio de técnicos a nível nacional, regional e internacional; b) A participação de nacionais em projectos internacionais sobre segurança cibernética; e c) O estabelecimento de centros de formação e pesquisa. 2. Programa de incentivo ao desenvolvimento de soluções cibernéticas estabelecido; e 3. Programa de estimulo e criação de *startups* estabelecido.
OE6- Criar programas e mecanismos de consciencialização sobre os riscos associados ao uso de espaços cibernéticos	
Código do Projecto: OE6-I21	
Iniciativa	Fóruns de discussão de matérias relacionadas à segurança cibernética a nível nacional
Descrição	Definir fóruns de discussão de matérias relacionadas com a segurança cibernética a nível nacional, que promovam a partilha de informação relacionada com este tema e estimular a participação de nacionais em fóruns e actividades internacionais sobre segurança cibernética
Entregáveis	1. Fóruns de discussão nacional sobre segurança cibernética estabelecidos; e 2. Mecanismos de estímulo à participação de nacionais em fóruns internacionais estabelecidos.
Código do Projecto: OE6-I22	
Iniciativa	Realizar um inquérito nacional de avaliação do nível de consciencialização dos Sectores público e privado e da sociedade civil

	em segurança cibernética
Descrição	Realizar um inquérito nacional para avaliar o nível de consciencialização dos Sectores público e privado e da sociedade civil em segurança cibernética para melhor definir as acções de elevação do nível de consciência sobre os ataques, por sectores e camadas sociais, crianças, jovens, mulheres e outros grupos mais vulneráveis.
Entregáveis	1. Indicadores a serem usados no inquérito estabelecidos; 2. Modelo de inquérito desenhado; 3. Modelo de recolha de informação estabelecido; 4. Procedimentos para o tratamento e disponibilização de informação estabelecidos; e 5. Relatórios sobre os resultados do inquérito disponíveis.
Código do Projecto: OE6-I23	
Iniciativa	Realizar campanhas de consciencialização sobre segurança cibernética com especial enfoque na protecção da criança e de outros grupos vulneráveis
Descrição	Com base no inquérito realizado, definir o tipo de campanhas de consciencialização sobre segurança cibernética a serem realizadas no sector informal e por grupos alvos da sociedade civil e moldes em que estas serão realizadas
Entregáveis	1. Plano e moldes para a realização das campanhas estabelecidos; 2. Conteúdos a serem transmitidos nas campanhas de consciencialização desenvolvidos; e 3. Campanhas de consciencialização realizadas a nível nacional.

8 Governação da Segurança Cibernética

A governação da segurança cibernética no país será efectuada pelo Conselho Nacional de Segurança Cibernética (CNSC), um órgão com a responsabilidade de zelar por questões de soberania nacional, numa perspectiva inclusiva e presidido pelo Presidente da República, sendo constituído por:

1. Membros permanentes:
   - ✓ Ministro que superintende a área da Defesa;
   - ✓ Ministro que superintende a área de ordem, segurança e tranquilidades públicas;
   - ✓ Dirigente Máximo dos Serviços de Segurança do Estado;
   - ✓ Ministro que superintende a área das Tecnologias de Informação e Comunicação;
   - ✓ Ministro que superintende a área da Justiça;
   - ✓ Ministro que superintende a área das Comunicações;
   - ✓ Ministro que superintende a área das Finanças;

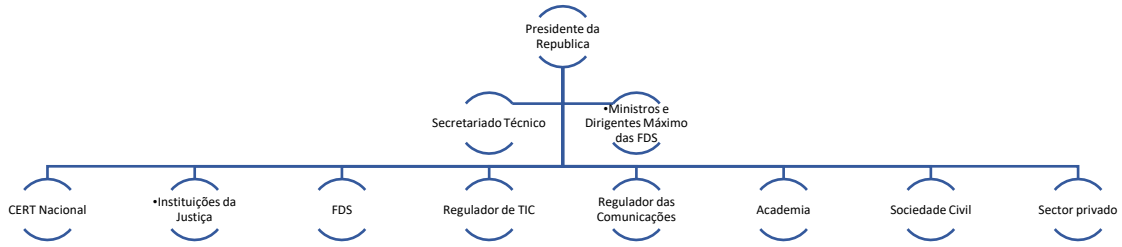
- ✓ Representantes das entidades reguladoras de TIC e Comunicações;
- ✓ CERT Nacional;
- ✓ Secretariado Técnico;

2. Membros convidados para questões de consulta:
   - ✓ Representante da Academia;
   - ✓ Representante do Sector Privado; e
   - ✓ Representante da Sociedade Civil.

O CNSC, deverá elaborar e aprovar os planos de execução anual, definir as fontes de financiamento das iniciativas a serem implementadas, assim como avaliar o cumprimento das iniciativas em curso. Este organismo ira avaliar continuamente o grau de cumprimento das iniciativas em curso e seu impacto, tendo como base a informação produzida pelas diferentes instituições intervenientes na implementação desta estratégia.

Para além de fornecer orientações políticas e estratégicas de alto nível, o CNSC terá também um papel importante na dinamização da implementação desta estratégia junto das áreas com influência directa para a sua materialização, assim como, irá assegurar que se evite a duplicação de esforços, que muitas vezes promove a incoerência das informações partilhadas pela multiplicidade de partes interessadas e relevantes nesta matéria, garantindo igualmente a privacidade, confidencialidade, integridade de indivíduos, instituições, dados e sistemas.

Figura 1: Estrutura do Conselho Nacional de Segurança Cibernética (CNSC)



8.1 Papel do CNSC

O Presidente da República, como comandante em Chefe das FDS assume o papel de líder do CNSC, na medida em que efectua o alinhamento de alto nível das políticas, estratégias e outros documentos orientadores para a defesa da soberania nacional, estando sobre a sua responsabilidade garantir que CNSC:

- ✓ Confira o alinhamento político e estratégico dos vários ministérios, governos provinciais ou outras entidades que estejam envolvidas na implementação da ENSC;
- ✓ Assegure que os documentos da PNSC, assim como a ENSC, sejam revistos, actualizados e alinhados com os desafios estratégicos de desenvolvimento do país;
- ✓ Certifique que sejam desenvolvidas normas, regulamentos, propostas de lei e outros instrumentos que assegurem a existência de um quadro legal adequado e apropriado para fazer face aos desafios impostos a exposição do Governo a espaços cibernéticos;
- ✓ Ateste o desenvolvimento de metodologias, regulamentos e outros instrumentos para assegurar uma coerente e uniforme implementação das soluções através das várias entidades;
- ✓ Verifique a avaliação dos riscos inerentes às estratégias desenhadas e propor soluções para a sua mitigação ou eliminação;
- ✓ Eleger as ICI e determinar as acções que visam garantir a sua protecção contra crimes e ataques cibernéticos;
- ✓ Avalie o estado nacional de Segurança Cibernética, determine as necessidades prioritárias e assegure as respostas apropriadas para cada caso;
- ✓ Acompanhe do progresso de implementação da ENSC pelas demais entidades envolvidas no processo;
- ✓ Confirme a aplicação de medidas correctivas em caso de desvios na implementação;
- ✓ Afiance a coordenação dos diversos actores relacionados com a segurança cibernética;
- ✓ Garanta a análise conjunta dos desafios enfrentados no combate aos crimes cibernéticos;
- ✓ Assegure a convergência de esforços e de iniciativas entre as instituições envolvidas e a actuação destas de forma complementar em todas as acções que serão executadas para garantir segurança do espaço cibernético nacional desde a criação de condições para a prevenção dos ataques, o recebimento de denúncias, o apuramento dos incidentes verificados, assim como a promoção da consciencialização e a educação da sociedade sobre os riscos a que estão expostos ao usarem as TIC;
- ✓ Confirme que sejam estabelecidos os indicadores de impacto que permitam avaliar o nível de execução, evolução e implementação das várias medidas e iniciativas propostas, para o estabelecimento dum espaço cibernético seguro e resiliente; e
- ✓ Ateste o desenvolvimento dum Observatório Nacional de Segurança Cibernética, contendo informação que permita auferir o nível de segurança cibernética do país, assim como o nível de consciencialização das instituições e do cidadão sobre os crimes cibernéticos e os mecanismos de prevenção, detenção, monitoria e resolução de crimes e conflitos cibernéticos estabelecidos.

A liderança desta matéria pelo Presidente da República é imprescindível, pois somente ela poderá agilizar todas as aprovações necessárias para a implementação dos projectos, assegurar a criação de todas as condições essenciais, para a salutar operacionalização dos planos a serem definidos no âmbito da implementação desta ENSC.

8.2 Papel dos Membros da CNSC

Os membros do CNSC, para além de assessorar o Presidente da Republica nas matérias de segurança cibernética relacionadas com as especificidades das áreas a que estão ligados, devem igualmente desempenhar os papeis descritos a seguir.

8.2.1 Os Ministros e Dirigentes Máximos das Forças de Defesa e Segurança

Os Ministros e Dirigentes máximos das FDS, são responsáveis por assegurar a implementação da presente estratégia nas suas áreas de jurisdição, garantindo que as iniciativas propostas nesta estratégia sejam implementadas com o devido zelo para proporcionar um espaço cibernético seguro no país, estando sobre a sua responsabilidade:

- ✓ Garantir a colaboração dos seus sectores nas matérias relacionadas com segurança cibernética com as demais instituições;
- ✓ Assessorar técnica e juridicamente, o CNSC e as instituições intervenientes na implementação desta estratégia, em matérias relacionadas com a segurança cibernética;
- ✓ Criar mecanismos para a viabilização de investimentos para a área de segurança cibernética, através de fundos públicos, privados e ou donativos;
- ✓ Assegurar a criação da capacidade institucional de todas as instituições chave para a garantia da defesa nacional, aos ataques e crimes cibernéticos;
- ✓ Promover a cooperação e coordenação intergovernamental em todos os aspectos inerentes a criação dum ambiente propício para responder a insegurança cibernética;
- ✓ Promover e encorajar parcerias público-privada para encontrar as melhores práticas e soluções de prevenção e resolução de conflitos resultantes de crimes cibernéticos;
- ✓ Assegurar o cumprimento das acções e dos objectivos específicos definidos na estratégia; e
- ✓ Definir e encontrar alternativas de financiamento para a implementação das iniciativas propostas nesta estratégia.

8.2.2 As Forças de Defesa e Segurança

As FDS têm a missão de proteger e garantir a segurança nacional, devendo para tal:

- ✓ Propor as condições técnicas que devem ser criadas nas instituições de defesa e segurança de modo a permitir que possam levar a cabo as actividades de investigação e responsabilização dos autores dos crimes cibernéticos que tiverem lugar no espaço cibernético nacional;

- ✓ Propor normas e medidas que garantam que as comunicações entre as instituições públicas se tornem mais eficazes e seguras;
- ✓ Sugerir medidas de prevenção, detenção, contenção e reação contra os incidentes ocorridos no ciberespaço nacional e garantir a segurança da sociedade e do Estado;
- ✓ Coordenar e executar a reação contra as acções ilícitas criminais praticadas contra as ICI, os activos de informação e responsabilizar criminalmente os autores dos delitos; e
- ✓ Articular as ações de deteção e contenção, trocando informações com as equipes de tratamento a incidentes de rede, de forma a obter informações dos ataques ou tentativas de ataques e das vulnerabilidades identificadas no sistema.

8.2.3 As Instituições de Justiça

- ✓ Garantir a colaboração dos seus sectores nas matérias relacionadas com segurança cibernética com as demais instituições;
- ✓ Assessorar juridicamente, o CNSC e as instituições intervenientes na implementação desta estratégia, em matérias relacionadas com a segurança cibernética;
- ✓ Fazer a revisão do quadro legal existente de modo a incluir nele os aspectos relacionados com a segurança cibernética;
- ✓ Propor medidas punitivas a serem adotadas nos diferentes crimes cibernéticos praticados, coerentes com os danos causados;

8.2.4 O Regulador de TIC

O Regulador de TIC, sendo o responsável pela elaboração da presente estratégia, deve assegurar em coordenação com CNSC, a implementação e monitoria dos vários projectos desempenhando os seguintes papeis :

- ✓ Orientar o Estado sobre assuntos e/ou outras matérias pertinentes que contribuam para a segurança cibernética;
- ✓ Propor um quadro legal e regulatório que promova a segurança cibernética no país;
- ✓ Propor um mecanismo de coordenação dos diferentes sectores envolvidos de modo a alinhar eficazmente as acções a realizar e obter os resultados esperados;
- ✓ Coordenar com todos os órgãos da Administração Pública a realização de iniciativas no âmbito da segurança cibernética;
- ✓ Verificar omissões respeitantes a implementação de iniciativas e estruturas de Segurança Cibernética e propor a reposição das mesmas;
- ✓ Coordenar a nível Nacional estratégias de respostas aos organismos internacionais sobre segurança cibernética;
- ✓ Elaborar estratégias para a criação de estruturas e políticas organizacionais nacionais e regionais adequadas para fazer face aos crimes cibernéticos.

- ✓ Garantir que sejam estabelecidos indicadores de desempenho que permitam avaliar o nível de desempenho de cada iniciativa a ser implementada no âmbito desta estratégia; e
- ✓ Em coordenação com o CNSC, o regulador de TIC deve monitorar o cumprimento dos prazos de cada uma das acções no âmbito da implementação da estratégia.

8.2.5 O Regulador das Comunicações

Caberá ao representante do regulador das comunicações:

- ✓ Propor medidas que garantam a segurança das comunicações efectuadas no espaço cibernética nacional;
- ✓ Contribuir no estabelecimento dum quadro legal e regulatório que promova a segurança cibernética no país;
- ✓ Trabalhar em coordenação com os diferentes sectores de modo a garantir o alinhamento eficaz das acções a realizar no âmbito da implementação desta estratégia.
- ✓ Em coordenação com o regulador das TIC, promover e realizar acções que concorram para o bom uso do espaço cibernético.
- ✓ Contribuir para garantir um elevado nível de protecção dos dados pessoais e da privacidade.
- ✓ Zelar pela manutenção da integridade e segurança das redes de comunicações públicas e dos serviços acessíveis ao público, incluindo as interligações nacionais e internacionais

8.2.6 O Secretariado Técnico do Conselho Nacional de Segurança Cibernética (STCNSC)

O Secretariado Técnico do CNCS, é a unidade de apoio técnico do CNSC, na planificação, coordenação e controlo da implementação da ENSC, devendo este ser coordenado pelo INTIC, como instituição com atribuições de elaborar e coordenar a implementação de medidas para a melhoria do ambiente de segurança cibernética no país. Dada a transversalidade da segurança cibernética, que requer uma estreita colaboração das acções a serem desenvolvidas em prol da segurança do ciberespaço do país, serão incluídos no STCNSC técnicos da área de regulação das telecomunicações, das FDS, da justiça, da finanças e CERT Nacional e o âmbito das suas actividades o STCNSC estará encarregue por:

- ✓ Apoiar técnica e administrativamente o CNSC na realização do seu papel;
- ✓ Garantir que toda a documentação a ser apreciada pelo CNSC seja disponibilizada atempadamente aos seus membros, para que seja apreciada antes da realização dos encontros;
- ✓ Assegurar o cumprimento das acções e dos objectivos definidos na estratégia;

- ✓ Preparar os relatórios sobre a avaliação do cumprimento das actividades descritas no âmbito da estratégia, para apreciação pelo CNSC;
- ✓ Criar um mecanismo de coordenação dos diferentes sectores envolvidos, de modo a garantir um alinhamento eficaz das acções e dos resultados esperados;
- ✓ Propor alternativas de financiamento das actividades relativas à implementação da estratégia para aprovação do CNSC; e

8.2.7 O CERT Nacional

O CERT Nacional, na qualidade de órgão nacional de coordenação das equipes de resposta a incidentes cibernéticos tem no seu papel as seguintes responsabilidades:

- ✓ Coordenar as acções de resposta a incidentes de segurança cibernética;
- ✓ Ser o ponto central de notificações de incidentes cibernéticos a nível nacional e internacional.
- ✓ Criar e manter o Observatório Nacional de Segurança Cibernética;
- ✓ Garantir a partilha de informação com vista a mitigação de crimes cibernéticos em Moçambique; e
- ✓ Em coordenação com o regulador da área de TIC, motivar e garantir a criação de CSIRT sectoriais.

8.2.8 A Academia

A academia desempenha um papel preponderante, para a criação de um ambiente cibernético seguro, cabendo a ela:

- ✓ Aconselhar ao CNSC as soluções mais adequadas para mitigar os incidentes cibernéticos que ocorrem;
- ✓ Promover debates no âmbito de segurança cibernética;
- ✓ Encorajar as pesquisas para mitigar ou solucionar problemas de segurança cibernética; e
- ✓ Desenvolver planos curriculares que permitam a especialização de quadro nacionais, em matérias relacionas com segurança cibernética.

8.2.9 O Sector Privado

O sector privado é um parceiro chave na implementação de soluções que visam a mitigação dos riscos de segurança cibernética, desempenhando o papel de:

- ✓ Aconselhar sobre produtos e serviços essenciais para assegurar a protecção de infraestruturas de Tecnologias de Informação(TI);

- ✓ Fornecer estratégias e arquitecturas de segurança, operações e abordagens de gestão de risco cibernéticos na prestação de dos vários serviços;
- ✓ Fornecer soluções para a mitigação de vulnerabilidade de segurança;

8.2.10 A Sociedade Civil

A sociedade civil desempenha um papel de relevo, cabendo a ela:

- ✓ Dinamizar a implementação de acções de sensibilização da sociedade no geral no que tange a matérias de segurança cibernética
- ✓ Desenvolver mecanismo de divulgação de risco e ameaças, com vista a precaução e mitigação de riscos cibernéticos

9 Cronograma, Orçamentação e Responsáveis pela Implementação das Iniciativas

CÓDIGO	INICIATIVA	RESPONSÁVEIS	INTERVENIENTES	PRIORIDADE	ORÇAMENTO 10^3 (MT)	PERÍODO
OE1-I01	Criar e institucionalizar o Conselho Nacional de Segurança Cibernética (CNSC)	MCTES	MF, PGR, MJCR, MTC, MEF, MCTES, FDS	Alta	200,00	2021
OE1-I02	Criar e institucionalizar a Equipa de Resposta a Incidentes Informáticos a Nível Nacional (CERT Nacional – National Computer Emergency Response Team)	INTIC	MF, PGR, MJCR, MTC, MEF, MCTES, FDS	Alta	10.000,00	2021
OE1-I03	Apoiar na criação de Equipas de Resposta a Incidentes de Informáticos (CSIRT - Computer Security Incident Responce Team), Sectorias e nas instituições com ICI e Activos de Informação	CERT Nacional	Todas as instituições envolvidas	Média	5.000,00	2021-2024
OE1-I04	Criar e institucionalizar o Centro de Operações de Segurança Cibernética a nível Nacional (SOC Nacional – National Security Operation Center)	INTIC/CERT Nacional	PGR,MJCR, MTC(INCM), MEF(CEDSIF), MCTES(INAGE) e FDS	Alta	200.000,00	2022-2024
OE1-I05	Desenvolver o Observatório Nacional de Segurança Cibernética	CNSC/CERT Nacional	INTIC, INCM, instituições com ICI e activos de informação	Alta	15.000,00	2022-2024
OE2-I06	Mapear as ICI de Moçambique, identificando os riscos e vulnerabilidades existentes e os incidentes de segurança cibernética que nelas ocorrem	CNSC	INTIC, INCM e todos operadores de ICI	Alta	25.000,00	2022 - 2023

OE2-I07	Estabelecer o modelo de colaboração entre as Equipes de Resposta a Incidentes de Segurança Cibernética a Nível Nacional.	CERT Nacional	INTIC, INCM e todos operadores de ICI	Alta	2.500,00	2022-2023
OE2-I08	Estabelecer os procedimentos para a auditoria das ICI	INTIC/INCM	Todos operadores de ICI	Alta	10.000,00	2022-2022
OE3-I09	Rever e harmonizar o quadro legal existente, incluindo nele matérias referentes a crimes de segurança cibernética	MJCR	PGR, MJCR, INTIC,INCM, MEF, e FDS	Alta	25.000,00	2022-2024
OE3-I10	Reforçar o quadro legal sobre Segurança Cibernética	INTIC	INCM,MJCR,MCTES, MTC, FDS	Alta	30.000,00	2021-2024
OE3-I11	Ratificar convenções internacionais sobre segurança cibernética	MJCR	INTIC, INCM, MCTES, MTC, MNEC,FDS	Media	2.000,00	2022-2024
OE3-I12	Assinar acordos de cooperação judiciária em matérias de cibercriminalidade	MJCR	INTIC, INCM, MCTES, MCT, MNEC,FDS	Média	3.000,00	2022-2024
OE3-I13	Promover e Divulgar o quadro legal sobre segurança cibernética	MJCR/INTIC.	INCM, MCTES, MCT, MNEC	Alta	8.000,00	2021-2024
OE4-I14	Estabelecer sistemas de alerta dos incidentes cibernéticos	CERT/SOC	INTIC, INCM PGR, MJCR, MTC, MEF, MCTES e FDS	Alta	8.000,00	2022
OE4-I15	Criar mecanismos filtragem e remoção de conteúdos ilegais	CERT/SOC/MJACR	INTIC, PGR, MJCR, MTC, MEF, MCTES e FDS	Alta	10.000,00	2021-2024
OE4-I16	Estabelecer programas de simulação dos incidentes de segurança cibernética	CERT/SOC	INTIC, INCM,PGR, MJCR, MEF, FDS, instituições com ICI e activos de informação	Alta	30.000,00	2022-2024

OE5-I17	Criar capacidade técnico-operacional de resposta à segurança cibernética no país	INTIC/CERT	PGR, MJCR, MTC, MEF, MCTES, FDS, Academia, Sector privado	Alta	45.000,00	2022-2024
OE5-I18	Desenvolver programas de capacitação e de criação de habilidades técnicas e operacionais em segurança cibernética	INTIC/CERT/	Academia, sector privado e todas instituições com ICI e activos de informação	Média	50.000,00	2022-2024
OE5-I19	Promover o desenvolvimento de pesquisas que busquem soluções inovadoras na área de segurança Cibernética	Academia/INTIC	Instituições de pesquisa e inovação	Média	20.000,00	2022-2024
OE5-I20	Estabelecer parcerias de colaboração técnica a nível local, regional e internacional na prevenção e no combate ao crime cibernético.	MCTES	INTIC, CERT Nacional e Instituições de pesquisa e inovação	Média	20.000,00	2022-2024
OE6-I21	Realizar um inquérito nacional de avaliação do nível de consciencialização dos Sectores público e privado e da sociedade civil em segurança cibernética	CNSC	INTIC, CERT, INCM, Sectores público, privado e organizações da sociedade civil	Média	15.000,00	2022-2023
OE6-I22	Realizar campanhas de consciencialização sobre segurança cibernética com especial enfoque na protecção da criança e de outros grupos vulneráveis	PGR/CERT	Confederação das associações económicas e a sociedade civil	Média	15000,00	2022-2023
OE6-I23	Definir fóruns de elevação do nível de maturidade dos Sectores público e privado e sociedade civil em segurança cibernética	INTIC/CERT	PGR, MJCR, MTC, MEF, MCTES, FDS, instituições com ICI e activos de informação	Média	30.000,00	2023-2024
				Total Geral	**578 700,00**	

10 MONITORIA E AVALIAÇÃO

A monitoria e avaliação da ENSC será efectuada pelo CNSC, cabendo ao INTIC como responsável para a implementação desta estratégia, fazer uma proposta das acções a serem eleitas anualmente, de acordo com as necessidades primordiais em segurança cibernética e com os recursos humanos e financeiros disponíveis. A proposta a ser elaborada deverá incluir, os indicadores de desempenho que servirão para avaliar o cumprimento das acções a realizar em cada ano. As acções a serem eleitas assim como os indicadores de desempenho a elas associadas, farão parte integrante do Plano de Monitoria e Avaliação a ser aprovado pelo CNSC.

O Plano de Monitoria e Avaliação (PMA) a ser aprovado pelo CNSC, deverá permitir a reprodução de relatórios precisos sobre os progressos alcançados e a identificação de lições aprendidas e desafios encontrados em todos os procedimentos de prevenção, reacção e mitigação dos ataques e crimes cibernéticos. Sendo os elementos-chave da abordagem de monitoria e avaliação, da presente ENSC os seguintes:

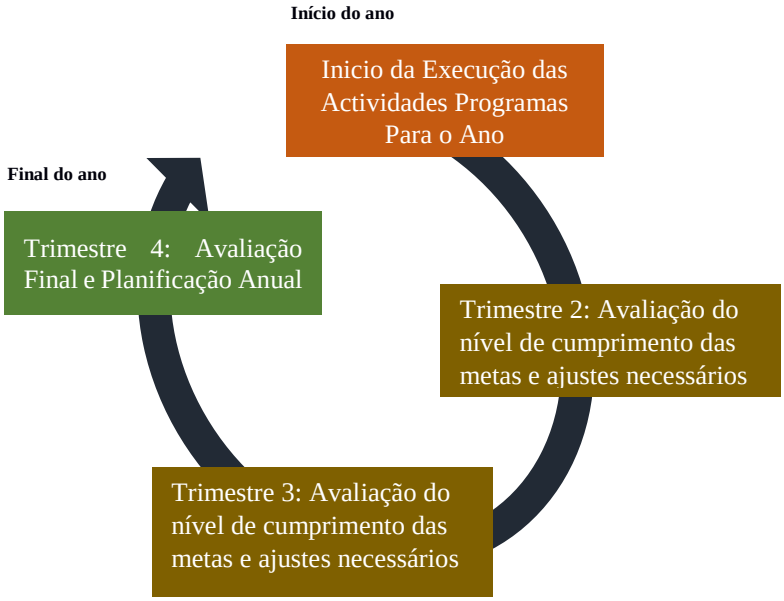
- ✓ O estabelecimento de metas de desempenho para as instituições governamentais ou partes interessadas responsáveis pela implementação das acções a serem eleitas anualmente da ENSC;
- ✓ O desenvolvimento de planos de desempenho que proporcionem uma compreensão partilhada dos resultados finais esperados, da abordagem levada a cabo para alcançar os resultados finais e a identificação dos recursos necessários para assegurar uma implementação bem-sucedida. Os planos basear-se-ão nos indicadores de desempenho a serem definidos em cada uma das iniciativas, nos resultados finais alcançados e no cumprimento dos prazos estabelecidos;
- ✓ A análise dos relatórios de desempenho e do progresso para a obtenção de resultados finais esperados; e
- ✓ A avaliação do desempenho institucional em relação às metas de desempenho estabelecidas.

O PMA, deve estar baseado na abordagem acima descrita e sua aprovação deverá acontecer num prazo máximo de três meses após a aprovação desta estratégia.

O plano de monitoria e avaliação permitirá avaliar as questões operacionais encontradas durante a implementação da estratégia, bem como a avaliação do impacto a longo prazo e dos resultados da estratégia com base em revisões periódicas. Fornecerá igualmente, mais detalhes sobre as ferramentas usadas na recolha de dados para a produção dos relatórios e

informações sobre os papéis e responsabilidades das partes interessadas, assim como a periodicidade da apresentação dos relatórios. Devendo o ciclo de monitoria da ENSC ser composto pelos seguintes estágios:

Figura 3 – Ciclo de Monitoria da ENSC



É na Planificação Anual, onde se deve realizar uma reunião anual de planificação e orçamentação das actividades a serem realizadas no ano seguinte, bem como definir as metas a atingir, alinhando-as com os indicadores de desempenho descritos no Plano de Monitoria e avaliação a ser aprovado pelo CNSC.

Trimestralmente será realizada a monitoria e avaliação do plano, visando aferir o grau de cumprimento da implementação das iniciativas, bem como definir as medidas correctivas necessárias de modo a alcançar os objectivos específicos definidos.

No final de cada ano será efectuada a análise anual, tendo como foco as actividades realizadas e a sua contraposição com os objectivos e metas definidas, obtendo assim uma avaliação do grau da execução destas e as eventuais dificuldades que possam existir na implementação do Plano de Actividades Anual. Face a esta avaliação poderão ser definidas medidas correctivas que serão incorporadas no Plano de Actividades do ano seguinte.

Complementarmente a estes momentos presentes no ciclo de monitoria anual, no final de 2024, ano final de implementação desta estratégia, far-se-á uma avaliação da execução e do impacto da estratégia e o balanço da implementação das iniciativas nos 4 anos que antecederam.

10.1.1 Matriz de Monitoria

Deverá ser desenvolvida uma matriz de monitoria com os principais indicadores a serem utilizados na avaliação da implementação das iniciativas propostas no âmbito desta ENSC, de modo a avaliar o impacto das iniciativas para a economia e para a sociedade.

10.1.2 Instrumentos de Suporte

A realização dos processos de monitoria e avaliação envolvem a recolha de dados fiáveis e relevantes, para tal será criado o Observatório Nacional sobre a Sociedade da Informação (ONSI) que conterá dados úteis e fiáveis sobre os registos de incidentes cibernéticos ocorridos no espaço cibernético nacional que possam servir de suporte à tomada de decisão política, estratégica e operacional assim como para a divulgação junto da sociedade civil.

11 Anexo

Glossário

Activo de Informação: tudo o que tem valor numa organização, podendo ser os meios de armazenamento, transmissão e processamento de informação, ou mesmo, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Ameaça cibernética: acto malicioso que visa destruir ou roubar dados ou perturbar o funcionamento normal dos sistemas computacionais.

Ataque cibernético: tentativa de *hackers* ou actores mal-intencionados de danificar ou interromper o funcionamento normal de uma rede, sistema ou aplicativo de computador.

Autenticidade: legitimidade da informação produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Ciberespaço: espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores a nível mundial.

Confidencialidade: assegurar que a informação é acessível somente às entidades devidamente autorizadas.

Cultura de cibersegurança: alinhamento da cibersegurança com os objetivos 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. 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.

Disponibilidade: garantir que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
Infraestruturas 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.
Infraestruturas Críticas da Informação: subconjunto de activos de informação que afectam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.
Integridade: garantia de que os dados permaneçam íntegros e sem qualquer alteração quando disponibilizados.
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 suscetibilidade 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.