ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA DE MOÇAMBIQUE

(PROPOSTA)

Versão 2

Conteúdo

1. SIGLAS E ABREVIATURAS

CERT Computer Emergency Response Team (Equipa de Resposta a Incidentes Informáticos)

ICI Infra-estrutura Crítica de Informação

ICT Information and Communications Technology (Tecnologias de Informação e Comunicação)

INTIC Instituto Nacional de Tecnologias e Informação e Comunicação

INCM Instituto Nacional das Comunicações de Moçambique

ISP Internet Service Provider (Provedores de Serviços de Internet)

R&D Research and Development (Investigação e Desenvolvimento)

MTC Ministério dos Transportes e Comunicações

M&E Monitoring and Evaluation (Monitoria e Avaliação)

MCTESTP Ministério de Ciências e Tecnologias Ensino Superior e Técnico Profissional

NCS National Cybersecurity Strategy (Estratégia Nacional de Cibersegurança)

PGR Procuradoria Geral da República

SERNIC Serviço Nacional de Investigação Criminal

SOP Standard Operating Procedures (Standards de Procedimentos de Operação)

2. DEFINIÇÕES

Cyberbullying

O termo ciberespaço descreve sistemas e serviços conectados, direta ou indiretamente, à Internet, telecomunicações e redes de computadores. A vida moderna depende do desempenho oportuno, adequado e confidencial do ciberespaço. Assim, a segurança cibernética é importante para todos os Estados, porque se esforça para garantir que o espaço cibernético continue a funcionar quando e como esperado mesmo sob ataque. A segurança cibernética já não é um problema de segurança de computador puro.

3. SUMÁRIO EXECUTIVO

A Estratégia Nacional de Segurança Cibernética de Moçambique (2017 - 2021), descreve a abordagem para assegurar que o país garanta um ciberespaço seguro e resiliente que seja utilizado com segurança pelo Governo, sector privado, sociedade civil e demais instituições. O Governo moçambicano tem como objectivo alavancar totalmente a banda larga e o ciberespaço para estimular o crescimento social e econômico e tornar o país numa sociedade baseada no conhecimento. Esta visão é consistente com a tendência global das TICs tornando-se um factor chave para o desenvolvimento social e económico de uma nação.

Actualmente, existe uma multiplicidade de ameaças e riscos que podem prejudicar o bom funcionamento do ciberespaço, incluindo os sistemas e serviços de TIC em Moçambique que podem provocar um impacto negativo nos esforços para o aproveitamento das TICs para o desenvolvimento socioeconómico.

Esta estratégia estabelece o compromisso do Governo de Moçambique em garantir um ciberespaço seguro e que contribua para o desenvolvimento socioeconómico. A presente estratégia estabelece a visão, missão, os objectivos estratégicos e objectivos específicos em relação ao ciberespaço. A estratégia também delineia as medidas ou acções que permitirão alcançar os objectivos e metas identificadas.

Assim, a presente estratégia está organizada da seguinte forma:

1. Siglas e abreviaturas.
2. Definições.
3. Sumário executivo.
4. Contextualização.
5. Princípios de orientação.
6. Estratégia.
7. Factores críticos de sucesso.
8. Mecanismos de Implementação.

Apêndice 1: apresenta o quadro de estruturas lógicas de implementação para a estratégia que inclui *Deliverables, Key Performance Indicators (KPI), Timeframes, Organizações Líderes e Opções de Financiamento.*

4. CONTEXTUALIZAÇÃO

4.1. Contexto Internacional

A tecnologia da informação revolucionou a maneira como vivemos e fazemos negócios. A convergência de tecnologias para ambientes inteligentes e ecossistemas integrados nos deixou vulneráveis. Isto tem sido acompanhado por uma ameaça crescente que não conhece limites: - ameaças cibernéticas.

Dado a sua característica transfronteiriça, nenhuma nação soberana ou corporação multinacional pode assegurar a segurança cibernética sozinho, exigindo uma abordagem conjunta, tanto dentro do país como a nível internacional

A resolução das Nações Unidas 56/183 (21 de Dezembro de 2001) aprovou a realização de uma Cimeira Mundial sobre a Sociedade de Informação em duas fases. A primeira fase realizada em Genebra aprovou uma Declaração de Princípios que permitiu estabelecer ideias básicas para uma Sociedade de Informação para todos, reflectindo todas as diferenças sem deixar de parte todos os interessados.

A segunda fase realizada em Tunis teve como objectivo pôr em movimento o Plano de Acção aprovado em Genebra e obter acordos no campo de Governança da Internet e mecanismos de financiamento para dar seguimento e implementação dos documentos aprovados nas duas fases da Cimeira.

A União Internacional de Telecomunicações, através da organização IMPACT (International Multilateral Partnership Against Cyber Threat), jogou um papel de liderança fornecendo sistemas de aviso prévio e treino aos especialistas de Segurança Cibernética em todo o mundo. Hoje a IMPACT tem acima de 152 países membros. A UIT desenvolveu na verdade uma estrutura nos países em desenvolvimento para ajudá-los a iniciar o processo de desenvolvimento de políticas e estratégias sobre segurança cibernética.

Em 2004 foi elaborado pelo Conselho da Europa com a participação de Canada, Japão, África do Sul e EUA a Convenção de Budapeste em Segurança Cibernética e que está aberta para qualquer país que desejem participar. A convenção é usada como uma directiva, padrão ou modelo em mais de 100 países.

4.2. Regional

Esforços a nível da SADC iniciaram em Novembro de 2012, quando os Ministros das TICs da SADC aprovaram as seguintes três Leis Modelo Harmonizadas para a Segurança Cibernética a nível da SADC: Lei de Comércio Electrónico, Proteção de Dados e Cibercriminalidade. Importa referir que estas leis-modelo foram desenvolvidas no âmbito do projecto HIPSSA (Harmonização das Políticas de TIC na África Subsariana) da União Internacional das Telecomunicações (UIT) e estão alinhadas com a Convenção da União Africana sobre Segurança Cibernética e Protecção de Dados Pessoais.

Dos países membros, todos já iniciaram a domesticação das Leis Modeladas Harmonizadas da SADC e tem como compromisso concluírem o processo até Dezembro de 2019, inclusive a criação dos CERTs nacionais. Com a assistência da UIT, países como Angola, Zimbabué e Moçambique iniciariam a elaboração dos termos de referência para o seus CERT, enquanto assistência técnica da CTO tem ajudado países como o Botswana a elaborar a sua estratégia nacional de segurança cibernética.

Assim, apenas as Maurícias e África do Sul concluíram este processo de criação de um quadro legal para proteger o espaço cibernético. As Maurícias já aprovaram a Lei de Uso Indevido de Computadores e Cibercriminalidade (CMCA) 2003; Lei de TICs em 2001; Lei de Transações Electrónicas em 2000 e Lei de Proteção de Dados em 2004. A Equipa de Resposta a Emergências Informáticas das Maurícias (CERT-MU) é o CERT nacional e coordena e trata as questões de segurança da informação a nível nacional desde 2008.

Semelhantemente, na África do Sul foi aprovado o Quadro Nacional de Política de Segurança Cibernética (NCPF) da África do Sul em 2012. O objetivo do NCPF é de criar um ambiente cibernético seguro, confiável que facilite a proteção de infra-estrutura crítica de informações, de segurança cibernética em apoio dos imperativos de segurança nacional e da economia.

4.3. Nacional

Moçambique tem estado a dar passos largos para criar um ambiente em que o cidadão tenha um acesso crescente as Tecnologias de Informação e Comunicação (TIC) e aos serviços associados. Acções a diferentes níveis tem contribuído para um crescente acesso a Internet e desenvolvimento de um ambiente em que as TIC são consideradas um instrumento que contribui

para uma melhor prestação de serviço tanto a nível do Governo bem como a nível do sector privado.

Como parte da implementação das estratégias de TIC e da administração pública acima referidas foram implementados muitos projectos no país. Abaixo são indicados alguns destes projectos que muito impulsionaram a Governação Electrónica em Moçambique:

- Projecto de Governo Electrónico e de Infra-estruturas de Comunicação de Moçambique (Mozambique Electronic Government and Communications Infrastructure -MEGCIP);
- Rede Electrónica do Governo (GovNet);
- Sistema de Informação do Pessoal do Estado (SIP);
- e-SISTAF (Sistema de Informação de Administração Financeira do Estado);
- Centros Provinciais de Recursos Digitais (CPRDs);
- Centros Multimédia Comunitários;
- Projecto e-BAU (Plataforma Integrada de Prestação de Serviços ao Cidadão)
- Projecto de Apoio a Melhoria de Qualidade e Proximidade dos Serviços Públicos dos PALOPs e Timor-Leste;
- Projecto de Formulários Electrónicos; e
- Projecto de Plataforma de Interoperabilidade.

É com esta visão que o Governo tem estado a desenvolver estratégias que garantam que o cidadão possa tirar um maior proveito das tecnologia e beneficiar-se de um serviço mais direcionado e de qualidade, através da implementação de sistemas e disponibilização de infraestruturas tecnológicas de prestação de serviço, desenvolvimento de políticas, leis, estratégias, e regulamentos no sector das TIC, que focalizam no desenvolvimento, modernização, cobertura geográfica, e redução de custos de acesso as infra-estruturas e serviços de telecomunicações nacionais.

O crescente acesso aos serviços das TIC, incluindo a Internet, é também acompanhado de crescentes vulnerabilidades a que o cidadão está sujeito e com isto também o crescimento dos crimes cibernéticos. O governo de Moçambique está também plenamente consciente da ameaça e dos efeitos negativos do crime cibernético sobre a sua nação e por isso tem sido feito esforços para garantir que hajam instrumentos que possam proteger o cidadão e penalizar os que cometem estes crimes com recurso as TIC. Estes esforços incluem:

- O novo Código Penal, Lei n.º 35/2014, promulgada em Dezembro de 2014, que cobre os crimes informáticos nos seus artigos 317, 318, 323, 324 e 326;
- A Lei 3/2017, a Lei das Transacções Electrónicas, promulgada em Janeiro de 2017, que visa proteger os consumidores e regular o uso de sistemas electrónicos no governo,sector privado e sociedade civil;
- Regulamento de controlo de Tráfego de Telecomunicações, Decreto n.º 75/214, de 12 de Dezembro;
- Regulamento de Registo de Cartões SIM, Decreto 18/2015;
- Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho.

Outrossim, tem-se notado que os diferentes esforços em curso, nalguns casos não se complementam fazendo que se criem lacunas na garantia da segurança cibernética, no combate ao crime cibernético e outros males a que estamos sujeitos no ambiente cibernético.É neste contexto que o Governo vê como uma necessidade primordial a elaboração de uma Estratégia Nacional de Segurança Cibernética que irá delinear o papel dos diferentes actores, para reduzir a vulnerabilidade das instituições e utentes da Internet. Esta estratégia irá indicar o papel dos diferentes sectores incluindo o Governo, a Banca, os prestadores de serviços, entre outros, em criarem mecanismos para minimizar os efeitos dos crimes cibernéticos no território nacional.

5. PRINCÍPIOS DE ORIENTAÇÃO

A Estratégia Nacional de Segurança Cibernética de Moçambique (ENSC) é sustentada pelos seguintes princípios orientadores:

i. **Legalidade:** A ENSC de Moçambique tem em conta as diversas leis em vigor em Moçambique e promoverá a protecção dos direitos, liberdades e garantias fundamentais dos moçambicanos.

ii. **Abordagem baseada em risco:**A ENSC adopta uma abordagem baseada em risco na avaliação de respostas as ameaças e riscos cibernéticos, assegurando a Segurança Cibernética em Moçambique.

iii. **Cooperação e Coordenação:** Esta Estratégia promove a coordenação e a cooperação entre as várias partes interessadas, tanto a nível nacional como internacional.

iv. **Responsabilidade partilhada e crime cibernético:** A ENSC reconhece a responsabilidade individual e partilhada de todos os utilizadores das TIC (indivíduos, sector privado e governo).

v. **Acesso universal ao espaço cibernético:** A ENSC procurará assegurar que todos os cidadãos moçambicanos devem ter acesso e poder utilizar o espaço cibernético de forma segura, independentemente da localização, género, raça, situação económica, entre outros.

6. REFERÊNCIAL ESTRATÉGICO

6.1. Visão

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

6.2. Missão

"Desenvolver a capacidade necessária e o ambiente de segurança cibernética que garanta um espaço cibernético seguro"

6.3.Objectivos Estratégicos

Para o alcance da visão e missão da ENSC, foram definidos 5 (cinco) objectivos estratégicos:

I. Melhorar a protecção da infra-estrutura crítica de informação (ICI).
II. Reforçar o quadro legal, técnico e operacional de segurança cibernética.
III. Estabelecer um quadro nacional para promover a partilha de informação, Cooperação e Coordenação em matéria de segurança cibernética.
IV. Desenvolver capacidade técnica de pesquisa e inovação em matéria de segurança cibernética.
V. Criar uma cultura nacional de segurança cibernética.

6.4.Objectivos específicos e acções

Nesta secção são detalhados os objectivos específicos e as acções necessárias para a concretização dos objectivos estratégicos:

I. Objectivo Estratégico (i): Melhorar a protecção da infra-estrutura crítica de informação (ICI)

É primordial que o Governo identifique e proteja as infra-estruturas críticas de informação, sobretudo porque os ataques e incidentes cibernéticos poderão causar danos a disrupção do funcionamento da economia nacional, incluindo a integridade da vida e saúde das pessoas. Os danos podem incluir o enfraquecimento da segurança territorial e da estabilidade do Estado, danos à reputação dos indivíduos e das instituições públicas e privadas moçambicanas. De facto, é imperativo que Moçambique priorize a segurança cibernética das suas ICI assegurando que estas ICI sejam seguras e resilientes.

A protecção das ICI e outras infra-estruturas de informação de Moçambique é uma responsabilidade partilhada de todos os utilizadores de TICs e requer a colaboração das partes

interessadas, sector público, privado e sociedade civil que possuem e/ou exploram infra-estruturas de informação. Todos deverão trabalhar em conjunto na avaliação dos níveis de segurança cibernética e as vulnerabilidades das infra-estruturas de informação de Moçambique e implementar medidas e/ou acções que atenuem ou resolvam ameaças e riscos cibernéticos actuais e futuros.

6.4.1. Objectivo específico 1

Gerir as ameaças à segurança cibernética para melhorar a resposta a incidentes

Acções:

- Estabelecer uma unidade governamental que coordenea segurança cibernética,envolvendo o sector privado e a sociedade civil;
- Criar o CERT Nacional;
- Estabelecer e actualizar o registo de incidentes de segurança cibernética;
- Avaliar e sugerir medidas para prevenir ou mitigar incidentes;
- Criar e executar de forma contínua cenários e programas de simulação de incidentes de segurança cibernética;
- Desenvolver e rever continuamente mecanismos para tratar dos riscos e ameaças à segurança nacional no espaço cibernético;
- Melhorar a capacidade das forças de defesa e segurança, para prevenir, detectar e reagir aos ataques cibernéticos.

6.4.2. Objectivo específico 2

Proteger as infra-estruturas críticas de informação de Moçambique

Acções:

- Identificar e mapear as ICI de Moçambique;
- Elaborar e actualizar um registo nacional de ICI;
- Realizar a monitoria, alertas, avaliação e testes regulares de ICI para detectar erros, vulnerabilidades e intrusões;
- Estabelecer e rever continuamente o Quadro Nacional de Governança da ICI, que descreve procedimentos e processos de protecção da ICI;

- Desenvolver e rever continuamente um Registo Nacional de riscos e vulnerabilidade, juntamente com osregulamentos e directrizes que promovam a avaliação e gestão contínua dos riscos nas ICI;
- Fazer auditorias regulares as ICI com vista a emitir recomendações para a sua protecção;
- Melhorar a cooperação internacional em matéria de protecção ICI.

II. ObjectivoEstratégico (ii): Reforçar o quadro legal, técnico e operacional de segurança cibernética

Espera-se que todos os utilizadores de TIC em Moçambique tomem medidas para garantir a sua segurança cibernética e combater o crime cibernético. Para tal, é necessário um ambiente propício que facilite os esforços dos utilizadores das TIC na garantia da sua segurança cibernética e na luta contra a criminalidade cibernética.

O Governo deve rever o quadro legal, técnico e operacional de segurança cibernética para garantir a prevenção, detecção e a repressão das actividades de criminalidade cibernética, a aplicação das leis relacionadas com a segurança cibernética e também orientar os utilizadores das TIC na adopção de práticas consistentes de segurança cibernética.

6.4.3. Objectivo específico 3

Reforçar o quadro legal para prevenção e combate ao crime cibernético

Acções:

- Ratificar as convenções internacionais sobre a segurança cibernética;
- Rever e harmonizar o quadro legal sobre crimes e segurança cibernética e desenvolver os instrumentos necessários para facilitar a sua aplicação;
- Divulgar o quadro legal sobre segurança cibernética.

6.4.4. Objectivo específico 4

Melhorar o quadro técnico e operacional relacionado com a segurança cibernética.

Acções:

- Implementar requisitos obrigatórios e mínimos de segurança e tecnologia para melhorar a protecção e resiliência das infra-estruturas das TIC;
- Desenvolver planos de contingência nacional que identifiquem prioridades de activos de resposta de emergência e procedimentos operacionais padrão;

- Mapear continuamente os recursos de resposta de emergência;
- Assegurar que os canais de comunicação estejam implantados para os casos de resposta a emergência;
- Reforçar a capacidade laboratorialde informática forense;
- Criar uma infra-estrutura de certificação digital e criptografia nacional e promover o uso, para estabelecer um ambiente seguro e confiável nos serviços de governo e comércio eletrônico;
- Criar condições para implementação a interoperabilidade dos sistemas informáticos sectorias com vista a minimizar a duplicação de esforços e recursos no âmbito da segurança cibernética;
- Assegurar a transição do protocolo IPV4 para IPV6 e disseminar amplamente informações sobre os benefícios da transição, incluindo os recursos de segurança IPV6 relacionados à confidencialidade, autenticação e integridade de dados.

III. Objectivo Estratégico (iii): Estabelecer um quadro nacional para promover a partilha de informação, cooperação e coordenação em matéria de segurança cibernética

Considerando a natureza sem fronteiras do espaço cibernético, bem como a sofisticação e complexidade das ameaças de segurança cibernética, para garantir a segurança do espaço cibernético requer um quadro de governação e institucional que promova a partilha de informação, coordenação e colaboração. Este quadro deve também evitar a duplicação e a incoerência dos esforços entre a multiplicidade de partes interessadas relevantes em Moçambique. O Governo procurará estabelecer medidas que promovam uma articulação entre o sector público, privado e sociedade civil a nível nacional e internacional com vista a garantir a segurança cibernética.

6.4.5. Objectivo específico 5

Reforçar a colaboração e o intercâmbio de informações sobre a segurança cibernética.

Acções:

- Desenvolver e rever continuamente um quadro nacional que gere o intercâmbio de informações, a colaboração e a coordenação em matéria de segurança cibernética;

- Desenvolver um programa que detalhe a colaboração internacional em várias áreas estratégicas de segurança cibernética, incluindo resposta a incidentes, capacitação, pesquisa e desenvolvimento, entre outras;
- Participar em fóruns e actividades internacionais sobre segurança cibernética;
- Estabelecer um fórum nacional anual para promover a partilha de informação em segurança cibernética;
- Nomear pontos focais nas instituições do Estado e privadas por forma a facilitar a interação e colaboração em matérias relacionadas com a segurança cibernética.

6.4.6. Objectivo específico 6

Reforçar a partilhade informações, coordenação e colaboração na prevenção e combate aocrime cibernético.

Acções:

- Desenvolver e actualizar continuamente uma estrutura de partilha de informação e colaboraçãoentre o sector público, privado e sociedade civil para a prevenção ecombateao crime cibernético;
- Reforçar a colaboração entre os Estados e parceiros regionais e internacionais na prevenção e combate ao crime cibernético;
- Criar e actualizar continuamente uma plataforma nacional *on-line*, acessível a todos os utilizadores de TIC, com informações relacionadas a ameaças, vulnerabilidades e incidentes cibernéticos.

IV. Meta Estratégica (iv): Desenvolver capacidade técnica de pesquisa e inovação em matéria de segurança cibernética

Tendo em conta as ameaças e ataques cibernéticos cada vez mais sofisticados e alinhados com a aspiração do Governo de ter uma economia digital baseada no conhecimento, o Governo reconhece que é crucial a capacitação de profissionais de segurança cibernética em todo o país, para garantir a capacidade de detectar, monitorar e abordar ameaças e incidentes cibernéticos.

6.4.7. Objectivo específico 7

Desenvolver e reforçar continuamente a capacidade técnica de segurança cibernética.

Acções:

- Desenvolver continuamente a capacidade técnica dos funcionários do Estado, para assegurar que sejam capazes de lidar eficazmente com incidentes cibernéticos cada vez mais sofisticados;
- Rever a agenda nacional de investigação para promover a pesquisa e desenvolvimento em segurança cibernética;
- Estabelecer centros nacionais de excelência para treinamento e pesquisa em segurança cibernética;
- Rever e actualizar o currículo de educação de nível primário, secundário e superior por forma a incluir matérias de segurança cibernética;
- Promover competições de inovação, projectos de pesquisa e desenvolvimento, novos programas de estudo e estágiosobre segurança cibernéticaem universidades e escolas;
- Incentivar as empresas nacionais para o desenvolvimento e fornecimento de serviços de segurança cibernética, bem como desenvolver actividades de pesquisa e desenvolvimentoem matéria de segurança cibernética;
- Promover a participação de instituições do Governo, do sector privado e da academia em projectos internacionais de pesquisa sobre segurança cibernética.

6.4.8. Objectivo específico 8

Adoptar mecanismos de recrutamento e retenção de técnicos especializados em matéria de segurança cibernética.

Acções:

- Criar carreira de regime especial para profissionais com especialidade na área de segurança cibernética;
- Identificar os requisitos de recursos humanosem segurança cibernética para as instituições operadoras de ICI;
- Capacitar regularmente os técnicos em matéria de segurança cibernética.

6.4.9. Objectivo específico 9

Aumentar a capacidade para prevenir, detectare reprimir os crimes cibernéticos.

Acções:

- Desenvolver cursos de *forense* digital para produção de provas,para detecção e repressão do crime cibernético;

- Formar os profissionais dasinstituições da justiça na interpretação e aplicação da legislação sobre segurança cibernética;
- Reforçar a capacidade das autoridades judiciárias para prevenir,investigar e sancionar crimes cibernéticos.

V.	**Objectivo Estratégico (v):** Criar uma cultura nacional de segurança cibernética.

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 indivíduos e instituições tomem medidas de segurança no espaço cibernético implementando boas práticas no usoda Internet. Além disso, o Governo entende que é responsável pela protecção das crianças e de outros grupos vulneráveis, incluindo a sua protecção na Internet, uma vez que não são capazes de fazê-lo. Crianças e outros usuários vulneráveis são geralmente vítimas de *cyberbullying*, solicitação sexual e *grooming*(aliciamento), pornografia infantil e outros conteúdos nocivos.

Esta Estratégia promove a implementação de várias medidas que permitam aos cidadãos e instituições a ter acesso a aconselhamento e informação sobre como protegê-los no espaço cibernético. Essas medidas também promoveriam uma cultura e uma mentalidade nacional de segurança aos cidadãos e instituições. A Estratégia também coloca um foco especial na criação de uma cultura e ambiente onde as crianças e outros grupos vulneráveis em Moçambique possam usar o espaço cibernético com segurança.

Alinhada à aspiração do Governo de criar uma economia digital em Moçambique, a estratégia também procura criar uma cultura e mentalidade em toda a nação que permita o pleno aproveitamento e o uso seguro do espaço cibernético, promova a confiança e aumento da utilização dos serviços de governo,transações e comércio electrónicos, conduzindo, consequentemente a um maior desenvolvimento social e económico de Moçambique.

6.4.10. Objectivo específico 10

Aumentar a consciencialização sobre a segurança cibernética no sector público, privado e sociedade civil.

Acções:

- Avaliar os actuais níveis de consciencialização sobre a segurança cibernética em todo o país;
- Implementar um plano nacional para aumentar a consciencialização sobre a segurança cibernética;
- Desenvolver e divulgar continuamente as melhores práticas de segurança cibernéticaa nível nacional;
- Promover a formação dos dirigentes das instituições nacionais sobre segurança cibernética.

6.4.11. Objectivo específico 11

Criar uma cultura de segurança on-line para crianças e outros grupos vulneráveis .

Acções:

- Criar e implementar programas nacionais e disseminar diretrizes para garantir a existência de conhecimentos e as competências necessárias sobre segurança cibernética nas crianças e outros grupos vulneráveis;
- Promover o uso de técnicas ou ferramentas de filtragem na Internet que impeçam o acesso de crianças e outros grupos vulneráveis a conteúdos prejudiciais;
- Encorajar os ISP e outros prestadores de serviços a consciencializarem os seus clientes, especialmente os pais e encarregados de educação, sobre como utilizar as ferramentas e tecnologias disponíveis para gerir os potenciais riscos para as crianças e outros grupos vulneráveis enquanto acedem aos serviços *on-line*.

7. MECANISMOS DE IMPLEMENTAÇÃO

7.1.Modelo organizacional

Em Moçambique não existe uma estrutura para a coordenação das políticas e intervenções de segurança cibernética a nível operacional e estratégico. Considerando que a garantia da segurança cibernética é material transversal e que abrange diferentes sectores da sociedade, há assim a necessidade de elaboração de uma abordagem integrada e coordenada em matérias relacionadas a segurança cibernética. Em resposta a tal necessidade, esta estratégia obriga o estabelecimento de um Conselho Nacional de Segurança Cibernética (CNSC) a nível estratégico.

7.1.1. CONSELHO NACIONAL SEGURANÇA CIBERNÉTICA (CNSC)

O Conselho Nacional de Segurança Cibernética porque vai tratar da segurança cibernética e esta matéria tocar com questões de política nacional, e o uso ilícito do ciberespaço poder prejudicar as actividades econômicas, saúde pública, a segurança nacional, logo fica claro o papel fundamental do Governo. Neste contexto, vê-se como primordial que o CNSC seja composto por dirigentes que superintendem as áreas que directamente contribuem para o funcionamento das TIC e a segurança dos cidadãos e da soberania Nacional, dirigidos por Sua Excia. o Presidente da República na qualidade de Chefe de Estado e Comandante e Chefe das Forças e Defesa Nacional.

A seguir são indicados os membros do CNSC:

- Ministro que superintende aárea da Defesa;
- Ministro que superintende aárea de ordem,segurança e tranquilidades públicas;
- Ministro que superintende a área da Justiça;
- Ministro que superintende a área das comunicações;
- Ministro que superintende aárea das tecnologias de informação e comunicação.

O papel do conselho é:

- Analisar e orientar o Estado sobre assuntos e/ou outras matérias pertinentes que contribuam para a segurança cibernética;
- Elaborar estratégias para a criação de estruturas e políticas organizacionais nacionais e regionais adequadas em matéria de crime cibernético.
- Assegurar a criação de capacidade institucional com vista a garantir a Defesa Nacional contra ataques e crimes cibernéticos;

- Promover cooperação e coordenação intergovernamental em matéria de Segurança Cibernética
- Promover e encorajar parcerias público-privada sobre assuntos relacionadas com a segurança cibernética no país;
- Avaliar o estado nacional de Segurança Cibernética, determinar as necessidades prioritárias e assegurar as respostas apropriada para cada caso;
- Eleger as ICI e determinar as acções que visem garantir a sua protecção contra crimes e ataques cibernéticos; e
- Verificar omissões respeitantes a implementação de iniciativas e estruturas de Segurança Cibernética.7

7.1.2. Unidade de coordenação e implementação da ECNS (U-ECNS)

A unidade de coordenação e implementação da ENSC é a unidade que se encarregará de assegurar o acompanhamento regular da implementação da estratégia, e nele farão parte todas as instituições ligadas directamente às acções definidas na matriz de implementação. No âmbito das suas actividades, será eleito uma entidade que se encarregará pela coordenação de todas as actividades.

O Papel da unidade é:

- Assegurar o cumprimento das acções e objectivos definidos na estratégia;
- Criar um mecanismo de coordenação dos diferentes sectores envolvidos na unidade com vista ao alinhamento eficaz das acções e resultados esperados.
- Definir e encontrar alternativas de financiamento das actividades relativas a implementação da estratégia.
- Monitorar o cumprimento dos prazos de cada uma das acções no âmbito da estratégia e assegurar que nenhum destes prazos são extrapolados.

7.2. Financiamento e Recursos

A implementação bem-sucedida do ENSC de Moçambique é totalmente dependente de financiamento e recursos adequados. Consequentemente, as estruturas lógicas de implementação daENSC detalhadas no Apêndice A deste documento detalham as possíveis organizações e fontes de financiamento para várias medidas propostas no ENSC.

Algumas das acções são ligadas ao funcionamento actual das organizações o que pressupõem simplesmente o melhoramento do seu funcionamento alinhado a segurança cibernética e protecção dos dados.

7.3. Monitoria e Avaliação

Uma estrutura de monitoramento e avaliação que apoie a realização da visão nacional de segurança cibernética e os objectivos estratégicos, permite relatórios precisos sobre o progresso e identificação das lições aprendidas e desafios encontrados é necessária para a implementação bem-sucedida do ENSC. Esta secção da estratégia descreve a abordagem nacional proposta para monitorar e avaliar o progresso na implementação do ENSC.

Os elementos-chave da abordagem de monitoramento e avaliação são:

- Estabelecimento de metas de desempenho para várias instituições governamentais ou partes interessadas relevantes responsáveis pela implementação de acções específicas daENSC;
- Desenvolvimento de planos de desempenho para estabelecer uma compreensão compartilhada dos resultados finais esperados, a abordagem para alcançar esses resultados finais e identificar os recursos necessários para assegurar uma implementação bem-sucedida. Os planos basear-se-ão nos KPIs, metas de desempenho e prazos fornecidos na Estrutura Lógica de Implementação;
- Monitoramento e relato de desempenho e progresso na obtenção de resultados finais esperados;
- Avaliação do desempenho institucional ou individual em relação às metas de desempenho estabelecidas
- Será encomendado a um interessado independente a realização da revisão intercalar e a longo prazo da estratégia para determinar o impacto a longo prazo e os resultados da estratégia com base em revisões periódicas e, se necessário, tomar medidas correctivas para manter a implementação no caminho certo. A revisão intercalar será realizada no final do primeiro trimestre do ano 2 da Estratégia e na revisão de longo prazo no final do 4º ano;
- A U-ENSC desenvolverá um Plano de Monitoramento e Avaliação abrangente, que será baseado na abordagem proposta, descrita acima, no prazo de três meses após a adoção da Estratégia.

- O plano de monitorização 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. O Plano de Monitoramento eAvaliação também fornecerá mais detalhes sobre as ferramentas para coleta de dados e relatórios, além de mais informações sobre os papéis e responsabilidades das partes interessadas e a frequência dos relatórios.

8. FACTORES CRÍTICOS DE SUCESSO

A ENSC por se tratar de um instrumento orientador sobre uma matéria transversal, critica e de abrangência nacional, necessita de uma liderança forte, financiamento, coordenação e colaboração, e de um monitoramento pontual e constante. Neste âmbito, vêm-se como factores críticos para o sucesso da implementação da estratégia os seguintes factores:

a) **Liderança:** Há que se definir uma liderança de alto nível do Governo, capaz de poder orientar os níveis de decisão e alinhar as acções de cariz nacional e de impacto à garantia da soberania nacional. Para o efeito, a liderança deve estar assente ao Presidente da República ou a quem ele indicar em sua substituição, através do Conselho Nacional de Segurança Cibernética.
b) **Monitoramento:** De forma regular esta ENSC deve ser monitorada, para tal dever-se-á ter em conta as responsabilidades e prazos constantes da matriz de acções. A U-ENSC deverá assegurar a coordenação e o monitoramento das acções sectórias realizadas.
c) **Financiamento:** Cada sector referido no âmbito da estratégia em termos de acções que contribuam para se atingir os objectivos definidos, deverão assegurar orçamentos com vista a suprir as necessidades de implementações das acções.
d) **Coordenação e colaboração:**O Sincronismo das acções entre os sectores deve ser assegurado por forma a que no final o conjunto de todas acções garantam a implementação efectiva da estratégia. Vê-se vital este sincronismo na medida em que a garantia da segurança cibernética ser somente possível de houverem acções transversais e de todos os sectores.

9. APÊNDICE

9.1.Matriz de Implementação e Orçamento

Esta secção apresenta os elementos-chave necessários para implementar com êxito a estratégia detalhada no capítulo 3 e incluem:

- Objectivo Estratégico: O objectivo substantivo a longo prazo que Moçambique gostaria de alcançar em cada área prioritária.
- Objectivo específico: as etapas específicas a serem adotadas para atingir seu objectivo estratégico.
- Acções: As actividades que devem ser empreendidas, no âmbito deste Plano Estratégico, na prossecução dos Objectivos Específicos.
- Entregas/Resultados: Os produtos de trabalho formal que Moçambique irá alcançar na prossecução dos objectivos e implementação da Estratégia.
- Entidadesimplementadoras: As instituições de Moçambique com a responsabilidade primária de gerir a conclusão de cada objectivo e as instituições que irão prestar apoio.
- Período de tempo: Período dentro do qual são produzidos os Produtos/Saídas e/ou as Estratégias/Acções são implementadas.
- Principais Indicadores de Desempenho: Os índices, medições de dados e tendências que devem ser monitorados para avaliar os progressos na implementação da Estratégia e na consecução dos objetivos e Resultados.
- Possíveis Fontes e Mecanismos de Financiamento: Uma visão geral das diferentes fontes de financiamento e mecanismos possíveis que podem ser adoptados por Moçambique para financiar a implementação do ENSC.

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
Objectivo Estratégico I –Melhorar a protecção da infra-estrutura crítica de informação (ICI)						
Proteger a infra-estrutura de informação crítica de Moçambique	Identificar e mapear as ICI de Moçambique;				Publicação do Registo Nacional CII	INCM/CERT de Moçambique
	Elaborar e actualizar um registo nacional de ICI;					
	Estabelecer e rever continuamente o Quadro Nacional de Governaça da ICI, que descreve procedimentos e processos de proteção da ICI				Publicação do Quadro Nacional de Governança da ICI que fornece detalhes sobre os procedimentos e processos de proteção da ICI	INCM/CERT de Moçambique
	Desenvolver e rever				Frequência dos	INCM/ CERT de

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	continuamente um Registo Nacional de Riscos, juntamente com as Regulamentações e Directrizes Nacionais que promovam a avaliação e gestão contínua dos riscos nas ICIs				exercícios de avaliação de riscos Frequência de actualização ao Registo Nacional de Riscos	Moçambique Moçambique CII
	Criar um Registo Nacional de Vulnerabilidade e estrutura para o monitoramento e divulgação regular de vulnerabilidades para a ICI	Registo Nacional de Vulnerabilidade e Estrutura de Divulgação de Vulnerabilidade para ICI			Frequência de atualização do registro de vulnerabilidades Frequência das divulgações de vulnerabilidade	INCM/ CERT de Moçambique CII

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Realizar a monitoria, alertas, avaliação e testes regulares de ICI para detectar erros e vulnerabilidades e intrusões;	Auditorias e testes de segurança para detectar erros e vulnerabilidades Sistemas de detecção de intrusão/exercícios			Número e frequência das auditorias e testes de segurança; Eficácia das auditorias e testes de segurança Eficácia dos testes/sistemas de detecção de intrusão;	CII
	Fazer auditorias regulares as ICI com vista a emitir recomendações para a sua protecção;					

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Melhorar a cooperação internacional em matéria de protecção ICI	Programa Internacional de Proteção CII Maior colaboração e mecanismos de partilha de informação & MOUs com parceiros internacionais sobre a monitorização, análise e gestão de CII transfronteiriças			Extensão da cooperação internacional na proteção da CII	MTC INCM/ CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
Monitorar e gerir continuamente ameaças cibernéticas e riscos para melhorar a resposta a incidentes	Criar uma unidade que coordena com os vários intervenientes que concorrem para a segurança cibernética					
	Criar o CERT nacional	CERT operacional com processos claros, funções e responsabilidades definidas			Extensão da operacionalização da CERT de Moçambique Eficácia da CERT de Moçambique	INCM/CERT de Moçambique
	Estabelecer e actualizar o registo de incidentes de segurança cibernética;	Registos atuais de incidentes de segurança cibernética; Medidas para prevenir / mitigar incidentes cibernéticos			Extensão das atualizações dos registros de incidentes; Extensão da implementação de medidas de mitigação	INCM/CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Avaliar e sugerir medidas para prevenir ou mitigar incidentes;					
	Criar e executar de forma contínua cenários e programas de simulação de incidentes de segurança cibernética;	Cenários e programas de simulação de incidentes de segurança cibernética			Utilização de cenários e programas de simulação de incidentes de segurança cibernética durante os exercícios nacionais	INCM/CERT de Moçambique
	Desenvolver e rever continuamente uma Estratégia Nacional de Defesa Cibernética que descreva a abordagem de Moçambique para	Planos de contingência nacionais (revistos regularmente)			Eficácia dos planos nacionais de contingência Extensão das revisões aos planos nacionais de contingência	INCM/CERT de Moçambique Forças militares /de segurança de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	tratar dos riscos e ameaças à segurança nacional no ciberespaço.					
	Aumentar a capacidade das autoridades das forças de defesa e segurança, para detectar e reprimir ataques cibernéticos;					
Objectivo Estratégico - 2: Reforçar o quadro legal, técnico e operacional de segurança cibernética						
Reforçar o quadro legal e para combater o crime cibernético	Ratificar as convenções internacionais sobre a segurança cibernética;					
	Rever o quadro legal sobre crimes cibernético e desenvolver os					

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	instrumentos necessários para facilitar a sua aplicação;					
	Criar uma legislação harmonizada na área de segurança cibernética;					
	Elaborar um código legal sobre segurança cibernética;					
	Avaliar e harmonizar o quadro legal nacional por forma a harmonizar com a legislação de outros países;					
	Divulgar o quadro legal sobre segurança cibernética a nível nacional;					

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
Melhorar o quadros técnicos e operacionais que promovem a segurança das CIIs, ISPs e outros usuários finais	Implementar requisitos obrigatórios e mínimos de segurança e tecnologia para melhorar a protecção e resiliência das infra-estruturas e sistemas dos ISP, ICI, sistemas governamentais de TIC e outros utilizadores, como o sector bancário, entre outros;	Requisitos mínimos e Obrigatório de tecnologia e segurança para equipamentos de ISPs e usuários finais			Extensão da identificação de equipamentos que não atendem aos requisitos mínimos de tecnologia ou segurança	INCM/ CERT de Moçambique CIIs, ISPs e outros usuários finais
	Desenvolver planos de Contingência Nacional que identifiquem prioridades de activos de resposta de	Plano Nacional de Contingência			Aprovação do plano nacional de contingência, incluindo as prioridades de recursos de resposta a emergências e procedimentos operacionais padrão	INCM/ CERT de Moçambique Foças de Defesa de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	emergência e procedimentos operacionais padrão (SOPs);				(SOPs)	
	Mapear continuamente os recursos de resposta de emergência	Mapa de ativos de resposta de emergência			Conclusão do mapa de ativos de resposta de emergência	INCM/ CERT de Moçambique Foças de Defesa de Moçambique
	Assegurar que os canais de comunicação estejam implantados para os casos de resposta a emergência.	Rede de Comunicação de Emergência			Extensão da implantação da Rede de Comunicação de Emergência	Provedores de Serviços de TICs/Comunica ões Forças de Defesa de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Criar um Laboratório Forense Digital.					
Objetivo Estratégico - 3: Estabelecer um quadro nacional para promover a partilha da informação, cooperação e coordenação em matéria de segurança cibernética						
Reforçar a partilha de informações, a coordenação e a colaboração no combate a criminalidade cibernética.	Desenvolver e actualizar continuamente uma estrutura de partilha de informação e colaboração entre o sector público, privado e sociedade civil para o combate a criminalidade cibernética;					
	Reforçar a colaboração com os Estados e parceiros regionais e					

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	internacionais no combate à criminalidade cibernética;					
	Criar e actualizar continuamente uma plataforma nacional on-line, acessível a todos os usuários de TIC, incluindo o sector público, privado e sociedade civil, com informações relacionadas a ameaças cibernéticas, vulnerabilidades e incidentes;					
Reforçar a colaboração e o intercâmbio de	Desenvolver e rever continuamente um quadro nacional que gere o intercâmbio de informações, a	Um quadro nacional que gere a partilha de informação, a colaboração e a			Extensão da colaboração, partilha de informação e coordenação a nível nacional	INCM MTC Ministério da Justiça

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
informações sobre a segurança cibernética	colaboração e acoordenação em matéria de segurança cibernética em Moçambique;	coordenação em matéria de segurança cibernética			Eficácia na troca e utilização de informações	
	Desenvolver um programa que detalha como Moçambique colabora internacionalmente em várias áreas estratégicas da segurança cibernética, incluindo resposta a incidentes, capacitação, pesquisa e desenvolvimento, entre outras	Programa que detalha como Moçambique colabora internacionalmente em várias áreas estratégicas da segurança cibernética Melhoria da colaboraçãointernacional			Eficácia e eficiência na colaboração internacional Extensão da colaboração e partilha de informação a nível internacional	INCM MTC
	Participar em todos os fóruns e actividades internacionais relevantes sobre	Melhoria da colaboração internacional em matéria de			Eficácia e eficiência na colaboração internacional	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	segurança cibernética	segurança cibernética Participação em todos os fóruns e atividades internacionais pertinentes sobre cibersegurança			Extensão da participação em todos os fóruns e atividades internacionais relevantes sobre segurança cibernética	
	Estabelecer um fórum nacional anual para promover a partilha de informação em segurança cibernética	Fórum Nacional de segurança cibernética			Nível de participação das partes interessadas nacionais no domínio da cibersegurança no fórum nacional	INCM MTC
Meta Estratégica - 4: Desenvolver capacidade técnica, de pesquisa e inovação em matéria de segurança cibernética						
Desenvolver e reforçar continuamente a	Desenvolver continuamente a capacidade técnica dos funcionários do Estado para assegurar que	Programa de Treinamento de CERT de Moçambique			Número e frequência das sessões de formação do CERT em	CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
capacidade técnica de segurança cibernética	sejam capazes de lidar eficazmente com incidentes cibernéticos cada vez mais sofisticados Uso da rede do Governo Uso de e-mails institucionais Promoção de desenvolvimento e uso do selo Made in Mozambique Promover a retenção do tráfico de internet Promover palestras educativas sobre a matéria em universidade e escolas -PKI -Maluana -Interoperabilidade				Moçambique; Número de incidentes/ataques/ameaças / riscos evitados /mitigados pela Equipe CERT	

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Rever a agenda nacional de investigação para promover a pesquisa e desenvolvimento em segurança cibernética;	Agenda Nacional Revista de Pesquisa que inclui os Aspectos de Segurança Cibernética			Extensão da implementação da Agenda Nacional Revista de Pesquisa que inclui os Aspectos de Segurança Cibernética	Ministério da Educação Academia MTC
	Estabelecer um Centro Nacional de Excelência para Treinamento e Pesquisa em Segurança Cibernética	Centro Nacional Operacional de Excelência em Cibersegurança Treinamento e Pesquisa			Extensão da operacionalização do Centro Nacional de Excelência	MTC Ministério da Educação Academia Sector privado
	Rever e actualizar o currículo de educação	Currículo de educação revisado que inclui aspectos			Extensão da implementação do currículo revisto	Ministério da Educação

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	de nível primário, secundário e superior por forma a incluir matérias de segurança cibernética;	sobre Cibersegurança				Academia
	Promover competições de inovação e projectos de pesquisa e desenvolvimento, novos programas de estudo e estágio sobre Cibersegurança em Universidades e Escolas	Programas de financiamento e incentivo para universidades envolvidas em R&D de segurança cibernética Competições nas escolas sobre segurança cibernética			Número de universidades participantes nos programas de financiamento	Programas de Incentivos Especiais fornecidos pelo Ministério das Finanças Ministério responsável pela Investigação Científica e pela Inovação; Academia; Ministério responsável pelo ensino superior

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
						Private Sector
	Apoiar as empresas nacionais no desenvolvimento e fornecimento de serviços de segurança cibernética, bem como desenvolver actividades de pesquisa e desenvolvimento em matéria de segurança cibernética;	Programas de financiamento e incentivo para as empresas nacionais que desenvolvem e fornecem serviços de segurança cibernética e desenvolvem actividades de R&D em matéria de segurança cibernética			Número de Empresas participantes no financiamento disponível e programa de incentivo	Programas de Incentivos Especiais fornecidos pelo Ministério das Finanças Ministério responsável pela Investigação Científica e pela Inovação; Academia; Ministério responsável pelo ensino superior
	Promover a participação de instituições nacionais	Novos estudos de nível superior e programas de estágio sobre			Número de novos estudos de nível terciário e programas de estágio sobre segurança	Ministério responsável pelo Emprego e Formação Profissional;

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	do Governo, do sector privado e da academia em projetos internacionais de pesquisa sobre segurança cibernética;	segurança cibernética			cibernética criados; Número de alunos / graduados matriculados em novos programas de estágio terciário e programas de estágio sobre segurança cibernética criados	Ministério da Educação Sector privado
	Promote the regular assessment of cybersecurity technical capabilities and needs across government institutions with a view Fortalecer as deficiências identificadas através da formação regular de pessoal de TI e outros funcionários relevantes dentro dessas	Regular assessment of cybersecurity technical capabilities and needs across Instituiçõesgovernamentais Planos nacionais de capacitação e treinamento de capacitação em Segurança			Number of assessments of cybersecurity technical capabilities and needs across Instituiçõesgovernamentais Número e frequência dos cursos / qualificações entregues / adquiridos Extensão de melhoria	Ministry responsible for Employment and Vocational Training INCM CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	instituições	Cibernética para Pessoal do Governo			em tecnologia. Capacidades	
Recrutar e adoptar mecanismos de retenção de quadros em matéria de segurança cibernética.	Criar a carreira de quadro de progressão na carreira e treinamento em segurança cibernética que promova o recrutamento e retenção de quadros de segurança cibernética, bem como o contínuo desenvolvimento e progressão de suas carreiras dentro de instituições governamentais e operadores de ICI;	Esquema de Progresso e Treinamento em Carreira Nacional de Segurança Cibernética que promove o recrutamento e retenção de profissionais de cibersegurança, bem como o contínuo desenvolvimento e progressão de suas carreiras			Extensão da implementação do programa de Progressão e Treinamento em Carreira Cibernética Extensão de recrutamento, retenção, desenvolvimento profissional contínuo e progressão na carreira de profissionais de cibersegurança em instituições governamentais e CIIs	Ministério responsável pelo Emprego e Formação Profissional; Ministério da Educação

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	Identificar os requisitos de recursos de segurança cibernética de agências governamentais e operadores de CII para priorizar áreas de recrutamento e retenção de profissionais de segurança cibernética	Conjunto de requisitos de recursos de segurança cibernética para agências governamentais e Áreas prioritárias para o recrutamento e retenção de profissionais de segurança cibernética			Extensão do recrutamento e retenção de pessoal em segurança cibernética	Ministério responsável pelo Emprego e Formação Profissional;
Aumentar a capacidade nacional para fazer cumprir as leis	Desenvolver cursos de forense digital e de produção de provas para os fazedores da justiça na aplicação da lei e pessoal de outras	Programa de treinamento em forense digital e manuseio de evidências			Número e frequência de cursos obrigatórios e qualificações entregues ou adquiridos em cibercrime por pessoal judiciário e de segurança em todo o	Polícia de Moçambique Ministério da Justiça,

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
relacionadas com a segurança cibernética, bem como detectar e reprimir os crimes cibernéticos.	instituições envolvidas na detecção e repressão do crime cibernético;				país Não de processos bem-sucedidos de cibercrimes	
	Formar os profissionais das instituições da justiça na interpretação e aplicação da legislação sobre segurança cibernética;	Programa de formação para reforçar a capacidade das agências de aplicação da lei e do judiciário na interpretação e execução dos quadros políticos,			Número de programas de capacitação realizados Capacidade de aplicação da lei e judiciário na aplicação dos quadros políticos, jurídicos e regulamentares sobre a	Execução da Lei e Judiciário

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
		jurídicos e regulamentares relevantes sobre a segurança cibernética em vigor em Moçambique Forte aplicação da lei e capacidade judiciária capaz de fazer cumprir os quadros políticos, jurídicos e regulamentares sobre a Cibersegurança em Moçambique			Cibersegurança em Moçambique Extensão da aplicação dos quadros políticos, jurídicos e regulamentares sobre a segurança cibernética	
	Aumentar a capacidade das autoridades judiciais para detectar e reprimir crimes	Programa de treinamento para aumentar a capacidade de			Número de programas de capacitação realizados	Execução da Lei e Judiciário

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	cibernéticos;	aplicação da lei e do judiciário para detectar e processar cibercrimes Forte aplicação da lei e judiciário capaz de detectar e processar cibercrimes			Capacidade de aplicação da lei e judiciário de detectar e processar cibercrimes Extensão da detecção e do julgamento de cibercrimes	
Meta Estratégica - 5: Criar uma cultura nacional de segurança cibernética						
Aumentar a consciencialização da segurança cibernética entre o público em geral e as instituições nacionais	Avaliar os actuais níveis de consciencialização sobre a segurança cibernética em todo o país e, consequentemente, desenvolver e implementar um plano nacional para aumentar	Avaliação nacional para verificar os actuais níveis de conscientização sobre a segurança cibernética Um plano nacional para melhorar o conhecimento da Cibersegurança em			Extensão da avaliação dos níveis nacionais de sensibilização para a segurança cibernética Dos níveis de consciência Número / frequência das campanhas de segurança cibernética	MTC INCM/CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	a consciencialização;	todo o país Site atualizado e funcional com informações actuais sobre ameaças, riscos, vulnerabilidades, etc; Campanhas de conscientização para aumentarem a conscientização sobre as tendências e ameaças da segurança cibernética			Eficácia das campanhas Número de revisões do website	
	Desenvolver e divulgar continuamente "Melhores Práticas Nacionais de Segurança Cibernética" para criar uma mentalidade de	Melhores práticas nacionais sobre segurança cibernética			Extent of dissemination of Cybersecurity Best Practices	INCM/CERT de Moçambique

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	segurança cibernética em todo o país					
	Promover a formação aos dirigentes das instituições nacionais sobre segurança cibernética.	Treinamento obrigatório de Conselheiros e Executivos de instituições nacionais sobre cibersegurança, especialmente CIIs e instituições públicas			Alcance dos conhecimentos dos Conselheiros e Executivos sobre Cibersegurança e como suas organizações lidam com ameaças e riscos cibernéticos	INCM/CERT de Moçambique CII
Criar mecanismos de colaboração intersectorial, incluindo o sector privado, para garantir que o espaço	Criar uma infra-estrutura de certificação de cerificação digital e criptografia nacional e promover o uso, para estabelecer um ambiente seguro e	Plano de implementação da PKI			Número de sistemas e aplicações de TIC do governo que incorporam o uso de PKI Número de serviços nacionais de comércio eletrônico que	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
cibernético apoie a partilha de informação, a pesquisa e desenvolvimento.	confiável nos serviços de governo eletrônico e comércio eletrônico; Criar condição para se implementar a interoperabildiade dos sistemas informáticos sectorias com vista a minimizar a duplicação de esforços e recursos no âmbito da segurança cibernética;				incorporam o uso de PKI	
	Assegurar a transição do protocolo IPV4 para IPV6 e disseminar amplamente informações sobre os benefícios da transição, incluindo os recursos	Plano de Implementação IPV4 para IPV6			Extensão da implementação do IPV4 para a Transição IPV6	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	de segurança IPV6 relacionados à confidencialidade, autenticação e integridade de dados;					
	Nomear pontos focais nas instituições por forma a facilitar a interação e colaboração em questões relaccionadas com a segurança cibernética.	Inspetores de Segurança Cibernética para apoiar pequenas e médias empresas na Cibersegurança			Grau de apoio prestado às PME	INCM
Criar uma cultura de segurança online para	Criar e implementar programas nacionais e disseminar diretrizes	Programa Nacional de Protecção das crianças e outros grupos vulneráveis			Grau de apoio prestado às PME Nível de implementação do Programa Nacional de	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
crianças e outros grupos vulneráveis	para garantir a existência de conhecimentos e as competências necessárias sobre segurança cibernética nas crianças e outros grupos vulneráveis;	on line			Proteção de Crianças e Outros Grupos vulneráveis on-line Proporção de famílias que tomaram medidas para manter as crianças e outros grupos vulneráveis seguros on-line	
	Promover o uso de técnicas ou ferramentas de filtragem na Internet que impeçam o acesso de crianças e outros grupos vulneráveis a conteúdos prejudiciais;	Orientações e melhores práticas para proteger as crianças e outros grupos vulneráveis das ameaças cibernética Utilização generalizada de			Frequência de publicação, revisão e atualização das melhores práticas e orientações Frequência de divulgação das melhores práticas e orientações	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
		medidas técnicas para impedir o acesso de crianças e outros grupos vulneráveis a conteúdos prejudiciais				
	Encorajar os ISP e outros prestadores de serviços a consciencializarem os seus clientes, especialmente os pais e encarregados de educação, sobre como utilizar as ferramentas e tecnologias disponíveis para gerir os potenciais	Programa Especial de Conscientização de Segurança on-line visando e informando Crianças e outros Grupos Vulneráveis. Conhecimento nacional e conhecimento de ferramentas /			Extensão da implementação do Programa Especial de Conscientização de Segurança On-line para Crianças e Outros Grupos Vulneráveis Número de Crianças e Membros de outros grupos vulneráveis com habilidades de como usar a Internet com segurança	INCM MTC

Objectivos Específicos	Estratégias/ Acções	Entregas/saídas	Entidades Implementadoras	Prazo	Indicadores Chave de Performance	Possíveis Fontes de Financiamento e Mecanismos
	riscos para as crianças e outros grupos vulneráveis enquanto acedem aos serviços online.	tecnologias que podem ser implementadas por ISPs e outros prestadores de serviços para manter as crianças e outros grupos vulneráveis seguros on-line;				