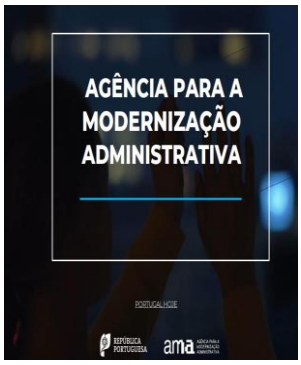
República de Moçambique

Ministério da Ciência e Tecnologia, Ensino Superior e Técnico Profissional

Instituto Nacional de Tecnologia de Informação Comunicação

Relatório da Participação na Reunião de Consulta de Comunidade de Especialistas Cibernéticos da Africa na Holanda e Visita de Trabalho em Portugal



22 a 25 de Novembro, 2011 – Holanda

26/11 a 3/12, 2021 - Portugal

Maputo, 29 de Dezembro de 2021

Índice

1. Introdução

O *Global Fórum on Cyber Expertise* (GFCE), é uma comunidade internacional com mais de 140 membros e parceiros de todas as regiões do mundo, estabelecida com o objectivo de fortalecer a capacidade e experiência cibernética a nível global. O GFCE pretende ser uma plataforma pragmática, orientada para ação e flexível para a colaboração internacional, contribuindo para reduzir a sobreposição e duplicação de esforços no ecossistema de desenvolvimento da capacidade cibernética (CCB), necessária para garantir um mundo digital aberto, livre, pacifico e seguro.

O GFCE, no âmbito das suas actividades, convidou o INTIC a participar na **Reunião de Consulta da Comunidade de Especialista Cibernéticos de África** em representação de Moçambique. O encontro teve lugar em Haia, na Holanda e decorreu de 22 a 24 de Novembro de 2021 com o apoio da fundação Bill & Melinda Gates. O encontro tinha como principais objectivos, o estabelecimento da comunidade de "Africa Cyber Experts (ACE)", que consistirá de especialistas cibernéticos de África que participarão na coordenação, envolvimento e apoio na implementação das actividades de capacitação cibernética no âmbito na iniciativa "Cyber Capacity Building (CCB)" em Africa. A comunidade ACE vai participar e contribuir para a concepção, desenvolvimento e implementação de módulos de conhecimento (KM).

A equipe do INTIC, durante a sua estadia em Haia, visitou o National Cybersecurity Center (NCSC-NL) que é parte integrante do Ministério da Justiça e Segurança, e que hospeda o CSIRT Nacional da Holanda. A visita tinha por objectivo colher experiência do modelo organizacional e identificar áreas de parceria com INTIC no desenvolvimento do CSIRT Nacional de Mocambique. Ainda nesta missão e na cidade de Haia, a equipa do INTIC parte desta missão reuniu com a equipe do projecto **Cyber Resilience for Development (Cyber4Dev)**, com o objetivo de estreitar as relações da parceria entre o INTIC e o Projecto Cyber4Dev.

O Projecto **Cyber Resilience for Development (Cyber4Dev)** é uma iniciativa da União Europeia concebido para promover a resiliência cibernética e a segurança cibernética, a fim de proteger as empresas públicas e privadas em todo o mundo. O Projecto Cyber4Dev tem por objectivo aumentar a resiliência cibernética de países do terceiro mundo, promovendo simultaneamente uma abordagem multisectorial e inclusiva baseada nos direitos humanos, garantindo o cumprimento do estado de direito e dos princípios da boa governação nos países participantes e beneficiários deste projecto. É de realçar que Moçambique eh um dos países beneficiários do Projecto Cyber4Dev.

A missão contemplava ainda uma visita de trabalho a Portugal, que decorreu de 27 a 29 de Novembro de 2021, onde estavam agendadas visitas e reuniões de trabalho com o Gabinete Nacional de Segurança (GNS), o Centro Nacional de Segurança Cibernética (CNSC), a Agencia para Modernização Administrativa (AMA), a Imprensa Nacional Casa da Moeda (INCM) e o Centro de Gestão da Rede Informática do Governo (CEGER), com o objectivo de colher experiência para dinamizar as acções relativas a implementação da Politica Nacional de Segurança Cibernética, em particular as acções ligadas a Operacionalização do

Sistema de Certificação Digital de Moçambique, o estabelecimento do CSIRT Nacional de entre outras actividades descritas na Estratégia Nacional de Segurança Cibernética bem como de iniciativas atinentes a modernização da administração pública com recurso a TICs.

2. Objectivos da Visita

A delegação do INTIC que se deslocou a Holanda e Portugal tinha por objectivo, i) participar do Comitê de Coordenação de Capacitação Cibernética da África (CCB), ii) desenvolver uma rede de contactos através da participação da reunião do comité e dos encontros bilaterais agendados, iii) colher experiencia e firmar acordos de parcerias para a implementação de acções concretos que permitam ao INTIC e ao pais como um todo, desenvolver mecanismos de combate ao cibercrime e melhorar a prestação dos serviços digitais ao cidadão enquadrados com a Estratégia Nacional de Segurança Cibernética recentemente aprovada pelo Governo, a Politica para a Sociedade de Informação e o Projecto de Governação Electrónica e da Economia Digital em Moçambique.

3. Composição da Delegação

A delegação moçambicana foi composta por 02 quadros do INTIC:

N/o	Nome	Instituição	Cargo ou Função
1	Prof. Doutor Eng. Lourino Alberto Chemane	INTIC	PCA
8	Eng. Sérgio Guivala	INTIC	Divisão de Segurança Cibernética e Proteção de Dados Pessoais

4. Visita a Holanda

4.1 Participação na reunião do GFCE.

A participação do INTIC na reunião de consulta da comunidade de especialista cibernéticos de africa, teve a duração de dois dias e a reunião estava centrada em três resultados principais:

i- Sistematização das Necessidades de Capacitação Cibernética (CCB) – com o objectivo de conduzir uma análise de linha de base das lacunas de CCB para identificar as necessidades prioritárias para os Estados Membros da União Africa (UA) no reforço da sua CCB nacional e resiliência cibernética.

ii- Desenvolvimento da Comunidade de "Africa Cyber Experts (ACE)" – com o obectivo de estabelecer uma comunidade de peritos africanos em cibersegurança selecionados entre os Estados membros da UA

participantes e outros afiliados da UA e grupo de várias partes interessadas do GFCE África.

iii- Desenvolvimento do Módulos de Conhecimento GFCE - Desenvolver módulos de conhecimento "Knowledge Module (KMs)" para capacitar os Estados membros da UA para melhor entender e enfrentar os desafios de capacitação cibernética.

Durante a reunião, os membros da comunidade ACE participaram de duas sessões principais a seguir apresentadas:

i. Sessão de Análise do CCB em África que cobriu:
   - Uma visão geral do projeto de colaboração AU-GFCE com foco no estado e no progresso alcançado.
   - Envolvimento e contribuição da Agência de Desenvolvimento da UA (AUDA-NEPAD).
   - Estado e análise do CCB da África e as lições aprendidas, com foco no resultado da análise do CCB e tendências nos estados membros UA.
   - Papel da comunidade ACE e sustentabilidade do projeto.

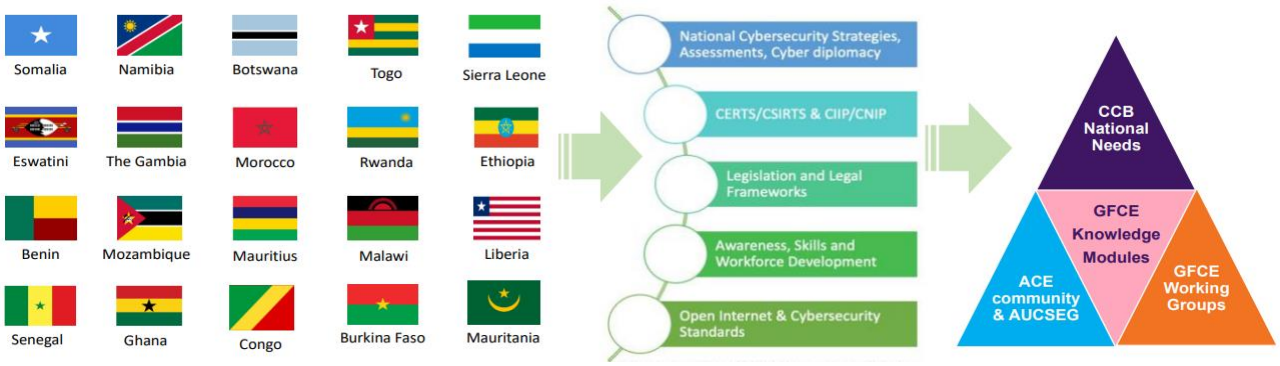
ii. Sessão do Módulo de Conhecimento (KM) da AU-GFCE que cobriu o desenho, desenvolvimento e implementação do KM. Esta sessão foi composta por grupos de discussão, conduzidos pela Fundação Diplo.

Durante as sessões os países membros partilharam informação e conhecimento especializado de seus países alinhados as áreas de foco do CCB, incluindo, mas não limitado a:

- Estratégia Nacional de Segurança Cibernética, avaliação da segurança cibernética, normas e diplomacia cibernética;
- CSIRTs/CSIRT; CIIP/CNIP;
- Legislação e Marcos Legais de segurança cibernética;
- Consciencialização, habilidades e desenvolvimento da força de trabalho;
- Padrões abertos de Internet e segurança cibernética.

Foram ainda sistematizadas e categorizadas as prioridades dos estados membro da UA no que tange ao desenvolvimento do CCB que se resumem na figura a abaixo

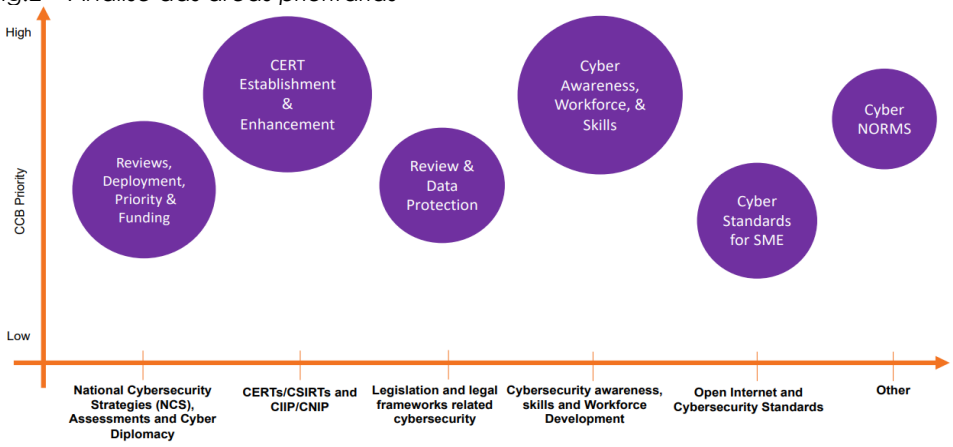
Fig.1 – Prioridade dos estados membros



Lições Aprendidas – a analise feita sobre "Cyber Capacity Building (CCB)" mostrou que o estabelecimento e melhoramento do CERT/CSIRT, a consciencialização, formação de equipes conjuntas de trabalho e a capacitação se mostraram de

alta prioridade para a maioria dos estados membros da UA. Outras áreas emergentes incluem a *Ciber diplomacia* e *ciber normas*. A Figura 2 apresenta os resultados da sistematização das lições aprendidas.

Fig.2 – Analise das áreas prioritárias



Acções de Seguimento

Moçambique pretende evoluir do seu estado de parceiro para o estado de membro deste projecto como forma de ter uma participação activa e melhor beneficiar o país e o continente.

Moçambique pretende acolher num futuro próximo o evento sendo que o mesmo será realizado na Cidade de Maputo.

O próximo evento será realizado em fevereiro de 2022 na cidade de Acra em Gana.

Impacto

Moçambique, como membro Comitê de Coordenação de Desenvolvimento de Capacidades Cibernéticas da África (CCB) que foi estabelecido para coordenar e supervisionar iniciativas e atividades de Capacitação Cibernética (CCB) em África, irá beneficiar do aumento da cooperação e engajamento que permitirá elevar a capacidade do país e do continente para mitigar os desafios enfrentados pelos estados membros da UA em relação às iniciativas do CCB e ataques cibernéticos ao país em particular e África no geral.

Por outro lado, como estado membro, eleva a probidade do país acolher uma das edições da reunião presencial dos estados membros, o que de certa forma ajuda na divulgação do pais e das suas potencialidades turísticas para além de representar uma oportunidade para o empresariado, da academia e da sociedade civil nacional beneficiar as acções no âmbito desta iniciativa.

Fig.3 – Sessão introdutória da reunião

4.2 Reunião com NCSC-NL

Este encontro visava colher experiência do Centro Nacional de Cibersegurança da Holanda (NCSC) e do respectivo CSIRT Nacional. Neste encontro foi feita uma apresentação sumária da estrutura funcional do Centro Nacional de Cibersegurança tendo sido feita a apresentação da plataforma de registo e solução de incidentes cibernéticos.

Lições aprendidas

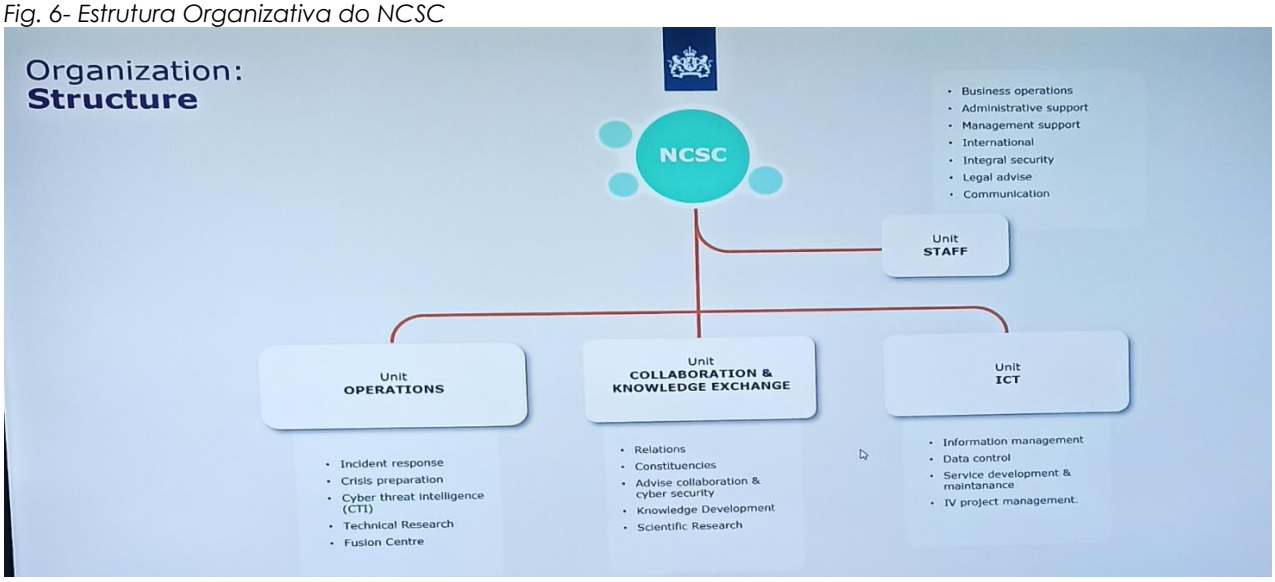
A Holanda adoptou uma estrutura da Rede Nacional de CSIRT baseada em sectores sendo que os sectores desenvolvem a sua própria rede de CSIRT porém, com mecanismos de partilha de informação e "*reporting*" para o Centro Nacional de Segurança Cibernética sem descurar da colaboração regional e Mundial. Moçambique vai trabalhar com a Holanda de modo a aprender do Centro Nacional de Cibersegurança da Holanda por o modelo de Rede Nacional de CSIRT ser similar ao aprovado por Moçambique no Estratégia Nacional de Segurança Cibernética.

Fig.4 – Ecossistema de segurança Cibernética Holanda

Fig.5 – Ecossistema de cooperação Internacional

O NCSC da Holanda (NCSC-NL) está dividido em três grandes blocos sendo um bloco Operacional, Um bloco que trata de questões de colaboração e troca de conhecimento e um bloco que trata da gestão de Informação, controle de dados e desenvolvimento e manutenção de serviços.

Fig. 6- Estrutura Organizativa do NCSC



Acções de seguimento

Prevê-se a assinatura de um plano de acão entre o INTIC e o NCSC-NL que cobre aspectos de legislação, treinamento e operação do CSIRT nacional.

Impacto

Desenvolvimento de competências técnicas para produção de instrumentos regulatórios na área de segurança cibernética assim como melhorar as competências técnicas para o estabelecimento, operação e manutenção do CSIRT Nacional de Moçambique e respectiva rede nacional de CSIRT.

4.3 Reunião com o Cyber4Dev

O objectivo do INTIC neste encontro visava estreitar os laços de pareceria com o Projecto Cyber4Dev a fim de beneficiar de assistência técnica, formação e prováveis financiamentos por parte deste projecto.

Neste encontro foi apresentado de forma sumária os objectivos do Projecto Cyber4Dev e foram identificadas as áreas onde o Projecto Cyber4Dev pode ajudar o INTIC na materialização da Estratégia Nacional de Segurança Cibernética recentemente aprovada pelo Governo.

Acções de seguimento

Será produzido e assinado um Plano de Accão entre o Projecto Cyber4Dev e o INTIC alinhados com a Política e Estratégia Nacional de Seguranca Cibernetica que ira incidir nas seguintes acções:

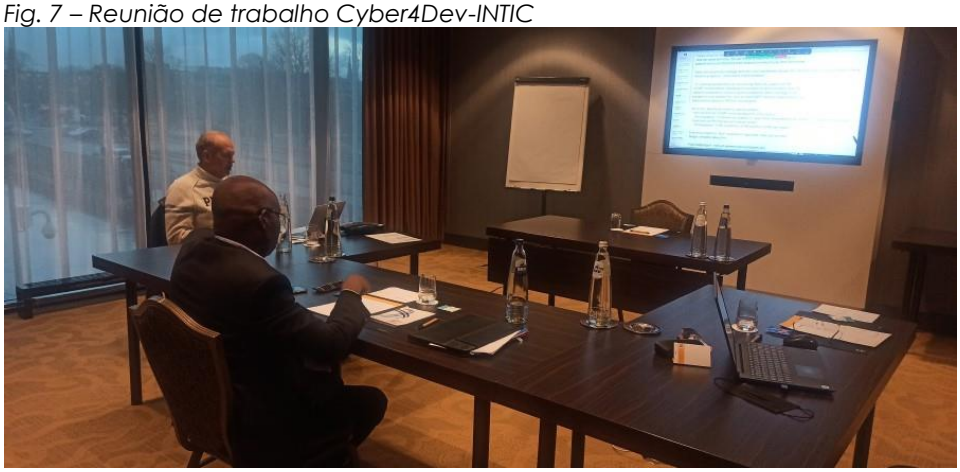
i- Realização de acções de formação e sensibilização em matérias de segurança cibernética incluindo formação de formadores,
ii- Apoio no estabelecimento do CSIRT nacional e da rede nacional de CSIRTs,

iii- Apoio na elaboração de directrizes e regulamentos atinentes a proteção de infraestruturas criticas;
iv- Apoio na realização de workshops sobre segurança cibernética.

Impacto

Sensibilização de dirigentes e cidadão comum em matérias de segurança cibernética, implementação de forma célere, do CSIRT nacional e elaboração de instrumentos normativos e regulatórios para as infraestruturas criticas de Moçambique.

Fig. 7 – Reunião de trabalho Cyber4Dev-INTIC



5. Visita a Portugal

A missão do INTIC contemplava ainda uma visita de trabalho a Portugal, que decorreu de 27 a 29 de Novembro de 2021, onde estavam agendadas visitas e reuniões de trabalho com o Gabinete Nacional de Segurança (GNS), o Centro Nacional de Segurança Cibernética (CNSC), a Agencia para Modernização Administrativa (AMA), a Imprensa Nacional Casa da Moeda (INCM) e o Centro de Gestão da Rede Informática do Governo (CEGER), com o objectivo de colher experiência para dinamizar as acções relativas a implementação da Politica Nacional de Segurança Cibernética, em particular as acções ligadas a Operacionalização do Sistema de Certificação Digital de Moçambique, o estabelecimento do CSIRT Nacional de entre outras actividades descritas na Estratégia Nacional de Segurança Cibernética bem como de iniciativas atinentes a modernização da administração pública com recurso a TICs.

Fig. 8 – Locais Visitados pelo INTIC na visita a Portugal

5.1 Reunião com CNCS

A visita ao GNS e ao CNSC tinha essencialmente dois grandes objectivos, sendo o primeiro de discutir mecanismos de partilha das boas práticas de estabelecimento e operação do Sistema de Certificação Digital, incluindo na operação do Sistema de Certificação Digital de Moçambique e rever o ponto de situação da implementação do plano de ação para áreas de colaboração no domínio da cibersegurança em curso, e aprofundamento das áreas de cooperação alinhadas com a Estratégia Nacional de Segurança Cibernética.

Lições Aprendidas

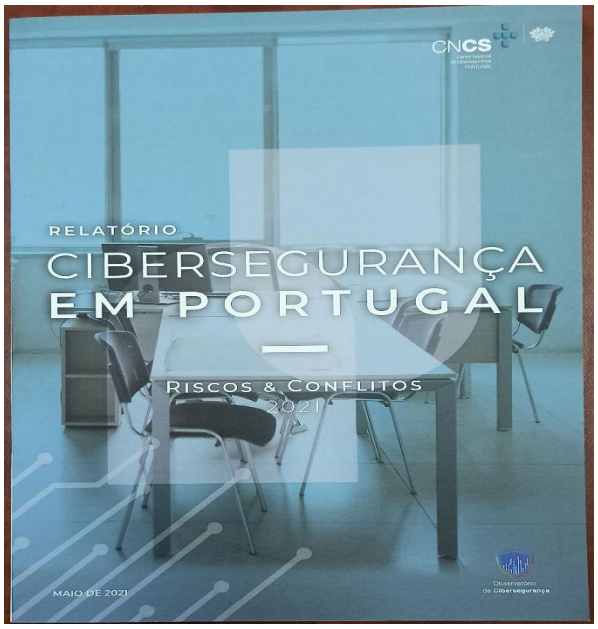
Todas as sessões temáticas foram de bastante interesse sendo de destacar dois a seguir apresentados:

1) **Observatório Nacional de Segurança Cibernética** de Portugal é uma plataforma de análise e sistematização de conhecimento em torno de temas multidisciplinares da cibersegurança, envolvendo as partes interessadas divididos em dois grandes grupos sendo um grupo de parceiros e outro o conselho consultivo.

   O observatório Nacional de Cibersegurança tem como produtos a publicação de relatórios sectorias, boletins, paginas web, Publicações temáticas, Modelos de análise e conferências/encontros. A Estratégia Nacional de Segurança Cibernética prevê a implantação de um Observatório Nacional de Cibersegurança de Moçambique e este aprendizado e parceria vai contribuir em grande escala na materialização deste objectivo.

Fig. 9 –Modelo de Governancal

Fig. 10 – Exemplar do relatório de Cibersegurança



2) **Acções de formação** visa fortalecer o factor Humano em três níveis sendo os utilizadores, os técnicos e os decisores usando uma abordagem integrada segundo ilustra a figura a baixo

Fig. 11 – Quadro estratégico de formação

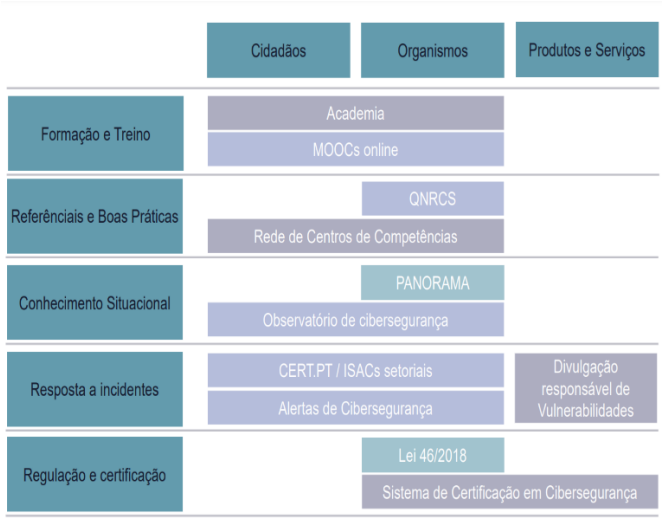


Fig. 12 – quadro do programa de sensibilização

A Estrategia Nacional de Seguranca Cibernetica preve o desenvolvimento de competecias e literacia digital em materia de seguranca cibertica pelo que este aprendizado ira contribuir em grande escala para a materializacao deste objectivo fazendo o uso dos conteudos programaticos que serao disponibilizados pelo CNSC ao INTIC.

Acções de seguimento

Ficou acordado que o GNS/CNSC e o INTIC irão assinar um acordo de parceria que será corporizada através do plano de acção acordado (em anexo), focado no apoio ao INTIC para a materialização da Politica e estratégia nacional de segurança cibernética priorizando as seguintes as seguintes acções:

i. Formação e capacitação de quadros do INTIC e outras entidades de Moçambique em matérias de segurança Cibernética fazendo o uso dos cursos e os respectivos conteúdos programáticos que serão cedidos ao INTIC como parte do acordo de parceria;
ii. Estabelecimento e operação da Equipe de respostas a Incidentes cibernéticos (CSIRT Nacional) e no estabelecimento da rede nacional de CSIRT;
iii. Estabelecimento do Centro Nacional de Operações de Segurança Cibernética (SOC Nacional);
iv. Desenvolvimento de mecanismos regulatórios e técnicos para a proteção das Infraestruturas Críticas de Informação (ICI) de Moçambique,
v. Apoio e colaboração no estabelecimento do Observatório Nacional de Segurança Cibernética de Mocambique; e
vi. Desenvolvimento e colaboração para realização de exercícios de simulação conjuntos de cibernética (CyberDrill) em Moçambique.

Impacto

As actividades identificadas terão um impacto na medida em que Moçambique passará a dispor de dados informativos e estatísticos relativos ao ambiente de segurança cibernética no país através do observatório nacional de segurança cibernética.

Os exercícios conjuntos de cibernética irão permitir ao nosso país identificar o seu nível de prontidão nas acções de resposta a incidentes massivos de segurança cibernética no pais e uma melhoria substancial nos mecanismos de detenção e proteção do espaço cibernético em Moçambique através da implementação do CSIRT nacional, da rede nacional de CSIRTs e do SOC nacional.

Fig. 13 – PCA do INTIC com o Presidente do GNS discutindo o quadro do programa de sensibilização

5.2 Reunião com AMA

A visita a Agência para Modernização Administrativa (AMA) tinha por objectivo partilhar a experiência Portuguesa no âmbito da modernização administrativa e transformação digital, com foco nas áreas da identidade digital, interoperabilidade, prestação de serviços digitais ao cidadão.

Durante a visita foi feita uma apresentação sobre o enquadramento institucional da AMA e projectos desenvolvidos no âmbito da modernização administrativa.

Acções de seguimento

Ficou acordado que será proposta a assinatura de um Memorando de Entendimento entre a AMA e o INTIC onde serão definidas as atividades concretas a realizar pela AMA, os objetivos a atingir e o calendário indicativo de atividades. O apoio da AMA cobrira os seguintes pontos:

i. Assistência técnica da AMA nos domínios da Identidade Digital que permita Moçambique implementar de forma célere sistemas de identidade digital para o cidadão Moçambicano.
ii. Apoio da AMA na implementação de um sistema centralizado de autenticação do cidadão e adopção de chave móvel digital em Moçambique.
iii. Apoio na Implementação do quadro de Interoperabilidade, ao abrigo do Projeto de Governação e Economia Digital em Moçambique, recentemente aprovado pelo Banco Mundial,
iv. A partilha de documentos de referencia de Portugal que concorrem para o estabelecimento célere de um quadro normativo e regulatório para o processo da modernização administrativa de Moçambique.

Neste âmbito foram partilhados os seguintes instrumentos que seguem em anexo:

1) As apresentações sobre Identidade Digital e Interoperabilidade, discutidas durante a reunião:
2) A apresentação institucional da AMA, com um panorama geral das atividades desenvolvidas por esta Agência nos eixos transformação digital; atendimento; e inovação & participação pública;
3) A Lei 36/2011, que estabelece a adoção de normas abertas nos sistemas informáticos do Estado e estabelece, no seu Artº 5, o Regulamento Nacional de Interoperabilidade Digital (RNID);
4) A Resolução do Conselho de Ministros 2/2018, que publica o RNID na sua revisão de 2018 (versão atualmente em vigor).

Impacto

Com esta parceria será possível dinamizar a operacionalização o quadro de interoperabilidade de Moçambique assim como implementar o sistema de identidade digital em Moçambique, em especial a plataforma de autenticação digital e a plataforma de assinaturas electrónicas, plataformas bastante importantes e facilitadoras do processo de modernização administrativa em Moçambique.

5.3 Reunião com INCM

Este encontro tinha por objectivo revisitar os termos e objectivos de contrato entre o INCM e o INTIC no âmbito da implementação do Sistema de Certificação Digital de Moçambique e identificar possíveis acções de seguimento para a operacionalização deste sistema e o respectivo sistema de recuperação de desastre.

Neste encontro foi passado em revista o contrato para a operacionalização do sistema de certificação digital de Moçambique com enfoque para a implementação do sistema de recuperação de desastre. O INCM referiu que devido a fuga de quadros, neste momento não tem capacidade técnica para manter e gerir o sistema de certificação digital instalado pelo que, será necessário rever todos os aspectos técnicos. As alterações a serem introduzidas aos ToRs, que serão elaborados com o apoio do CNCS, GNS, AMA, da Universidade da Santa Catarina no Brasil, da RNP e do INTIC do Brasil, entidades com as quais o INTIC está no processo avançado de estabelecimento de parcerias, irá contribuir para o melhoramento e operacionalização do SCDM.

Acções de seguimento

No âmbito da revisão da proposta técnica e tendo em conta as limitações financeiras do INTIC neste momento, ficou acordado que o INCM vai rever a proposta, focando-se na operacionalização do sistema ora instalado, sendo que o processo de implementação do sistema de recuperação de desastre será remetido a um concurso publico a ser financiado pelo Banco Mundial.

A segunda opção, em função da disponibilização de fundos do INTIC no Orçamento do Estado de 2022 e dada a urgência na operacionalização do SCDM, será a de o INTIC assinar uma adenda ou um segundo contrato com INCM para a implementação da acções urgentes de activação de duas entidades de certificação digital de segundo nível , uma do CEDSIF e outra do INAGE (MoRENet) que permita o inicio de prestação de serviços de autenticação digital e de assinaturas electróncias de forma piloto pelos utilizadores do eSISTAFE e pelos membros das comunidades académicas e cientificas de Moçambique, durante o primeiro trimestre de 2022.

5.4 Reunião com CEGER

O Objectivo deste encontro visava colher a experiência do CEGER na implementação de serviços de certificação digital ao Governo de Portugal.

O CEGER é o suporte tecnológico ao Governo de Portugal, assegurando a gestão da Rede Informática do Governo (RInG) e a prestação de todo o suporte necessário nos domínios das tecnologias de informação e de comunicações. O CEGER tem competência para exercer as funções de entidade certificadora, no âmbito do Sistema de Certificação Electrónica do Estado (Infraestrutura de Chaves Públicas - SCEE) para assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte e assinaturas electrónicas nas relações eletrónicas de pessoas singulares e coletivas com o Estado e entre entidades públicas.

Ações de seguimento

Será proposto a assinatura de um Memorando de entendimento entre o CEGER e o INTIC com enfoque para as seguintes áreas:

i. Apoio na operacionalização do sistema de certificação digital do estado;
ii. Apoio na implementação de sistemas de autenticação de dirigentes do estado através de sistemas de certificação digital e identidade digital;
iii. Apoio na Implementação de um sistema que permita os funcionários do estado assinarem digitalmente documentos;

Pela sensibilidade das áreas de intervenção do CEGER e do INTIC na área de segurança cibernética e de certificação digital do Estado, a assinatura do MoU entre o INTIC e o CEGER terá que ser aprovado pelas tutelas dos dois países.

Fig. 14 – Exemplar do Kit de cartão digital de dirigentes do Estado

Impacto

A curto médio prazo será possível, através desta parceria, fazer o uso do sistema de certificação digital para a criação de cartões caracterizados e personalizados que permitam a autenticação de dirigentes bem como a implementação de assinaturas digitais seguras para os dirigentes em Moçambique.

6. Resultados da Visita

#	INSTITUIÇÃO	RESULTADOS	IMPACTO	PERÍODO PROVÁVEL ADA IMPLEMENTAÇÃO	OBS
1	Fórum Global de Especialistas de Cibernética (GFCE)	Filiação de Moçambique como Membro do GFCE	Maior acesso a rede de especialistas de Segurança cibernética e participação activa no fórum	Abril de 2022	
2	Centro Nacional de Segurança Cibernética da Holanda (NCSC)	Assinatura de memorando de Entendimento entre o INTIC e o NCSC para operacionalização do CSIRT nacional	Celeridade e melhorias na implementação e operação do CSIRT Nacional.	Maio de 2022	
		Disponibilização dos conteúdos programáticos para formação em matéria de segurança Cibernética	Formação e sensibilização dos dirigentes do pais, quadros do Estado e do governo e cidadão no geral em matérias de segurança cibernética	Junho de 2022	
3	Cyber4Dev	Assinatura de um plano de acção	Maior apoio na Implementação e	Fevereiro de 2022	

		para o apoio na materialização da Estratégia Nacional de Segurança Cibernética	operação do CSIRT nacional, Maior apoio na realização de acções de formação e sensibilização em Segurança cibernética	
4	GNS/CNSC	Assinatura de acordo de parceria entre o GNS/CNCS e o INTIC	Formação de quadros Moçambicanos, melhoria do ambiente de segurança cibernética através do apoio na implementação do CSIRT, SOC e Observatório nacional de segurança cibernética e apoio na elaboração de leis, regulamentos e directrizes na área de segurança cibernetica	Fevereiro 2022
5			Apoio e celeridade na Implementação de Serviços Digitais para o Estado e o cidadão.	Abril 2022
	Agencia para Modernização Administrativa	Assinatura de acordo de parceria entre a AMA e o INTIC	Apoio na Implementação do sistema de Chave Móvel Digital	Agosto de 2021
			Apoio na Operacionalização do quadro de Interoperabilidade de Moçambique	Fevereiro 2023
6	INCM	Acordado a revisão da proposta técnica e financeira para a operacionalização do SCDM	Operacionalização a curto espaço da CA raiz do estado e reavaliação das especificações técnicas do equipamento existente	Fevereiro de 2022
7	CEGER	Assinatura de um MoU entre o CEGER e o INTIC/INAGE	Celeridade na Implementação do sistema de certificação do estado, celeridade na atribuição de Identidade digital a altos membros do Governo	Março de 2022

7. Conclusão

No computo geral conclui-se que a visita aos dois países foi bastante proveitosa na medida em que foi possível alcançar os objectivos planificados que concorrem para o desenvolvimento de competências e mecanismos de combate ao cibercrime, a melhoraria da prestação dos serviços digitais aos cidadãos, enquadrados com a Estratégia Nacional de Segurança Cibernética, a Politica para a Sociedade de Informação e o Projeto de Governação e Economia Digital em Moçambique.

É de realçar que dos resultados dos encontros realizados e das visitas de trabalho parte deste relatório constata-se que urge a necessidade de materializar a assinatura dos acordos e/ou memorandos de entendimento parte deste relatório e que sirvam de base para uma maior cooperação e materialização das actividades concretas identificadas.

É de destacar a disponibilidade de todas as entidades com as quais a delegação do INTIC reuniu e visitou em cooperar com Moçambique na materialização da agenda de TICs do país na área de segurança cibernética e certificação digital tendo se disponibilizado a receberem quadros do INTIC para estágios e no envio de seus especialistas para accoes de formação (*on-the-training*) no INTIC em projectos e iniciativas concretas referidas neste relatório.

A implementação das acções de seguimento e o impacto previsto em cada uma das visitas ou reunião com parceiros vai contribuir para a dinamização das acções prioritária parte da Estratégia Nacional de Segurança Cibernética e do Plano Estratégico da Sociedade de Informação de Moçambique.

Maputo, 29 de Dezembro de 2021

Anexos:

1. Relatório da Reunião do Comité – GFCE;
2. Agenda da Reunião com GNC/CNSC;
3. Propota de Plano de Actvidades entre o INTIC e GNC/CNSC; e
4. Agenda da Reunião com a AMA.