INTIC,IP
Instituto Nacional de Tecnologias de Informação e Comunicação
Autoridade Reguladora de Tecnologias de Informação e Comunicação

Cerimonia de Lançamento da Pagina Web e dos Serviços do CSIRT Nacional (nCSIRT.MZ-CC)

Apresentação do CSIRT Nacional e seus serviços

Maputo, 06 de Abril 2023

Conteudo

I. Contextualização.

II. Rede Nacional de CSIRTs

III. CSIRT Nacional:

- Serviços do CSIRT Nacional
- Cooperação Internacional
- Oportunidades de formação
- Actividades em curso
- Mecanismos de notificação de incidentes
- Conheça a nossa pagina

Contextualização

A Politica e Estratégia Nacional de Segurança Cibernética foi Aprovada em Agosto de 2021

BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

12.º SUPLEMENTO

IMPRENSA NACIONAL DE MOÇAMBIQUE, E. P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República»**.

SUMÁRIO

Conselho de Ministros:

Resolução n.º 69/2021:

Aprova a Política de Segurança Cibernética e Estratégia da sua Implementação.

Política de Segurança Cibernética e Estratégia da sua Implementação

1. Introdução

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

Para efeitos do presente documento entende-se por espaço cibernético ao ambiente complexo, de valores e interesses, materializado numa área de responsabilidade colectiva, que resulta da interacção entre pessoas, redes e sistemas de informação, e por segurança cibernética ao conjunto de medidas e acções de prevenção, monitorização, detecção, reacção, análise e correcção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no espaço cibernético, e das pessoas que nele interagem. A segurança

Somos todos chamados a participar de forma activa na implementação da PENSC como forma de Prevenir ataques e incidentes cibernéticos

Contextualização

A segurança cibernética é uma responsabilidade de toda sociedade, por isso, não é possível garantir a segurança cibernética do pais trabalhando de forma isolada;

É importante apostar na prevenção, consciencializando da sociedade para adopção de boas práticas e criar mecanismos de coordenação, como os CSIRTs Sectoriais e Institucionais e a respectiva Rede Nacional de CSIRTs para a coordenação e partilha de informação e ajuda mútua;

É necessário reforçar o quadro legal sobre segurança cibernética, com a elaboração de instrumentos legais e regulamentares, em paralelo com a introdução de mecanismos técnicos e desenvolvimento de capacidades para o estabelecimento de um ecossistema seguro;

Contextualização

Pilares do desenvolvimento da capacidade nacional de ciber defesa

- Lei de Cibersegurança
- Ciber defesa
- Lei de Ciber Crime
- Protecção Infraestruturas Criticas
- Ciber Diplomacia
- Literacia Cibernética

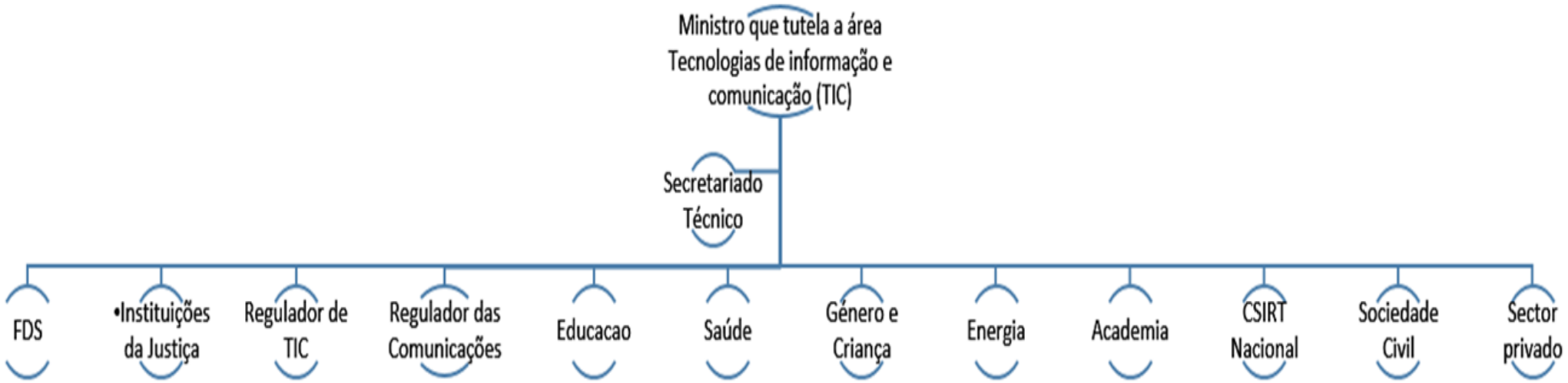
Os desafios da sociedade para dar resposta as ameaças cibernéticas

Contextualização

Governação e Coordenação da Segurança Cibernética

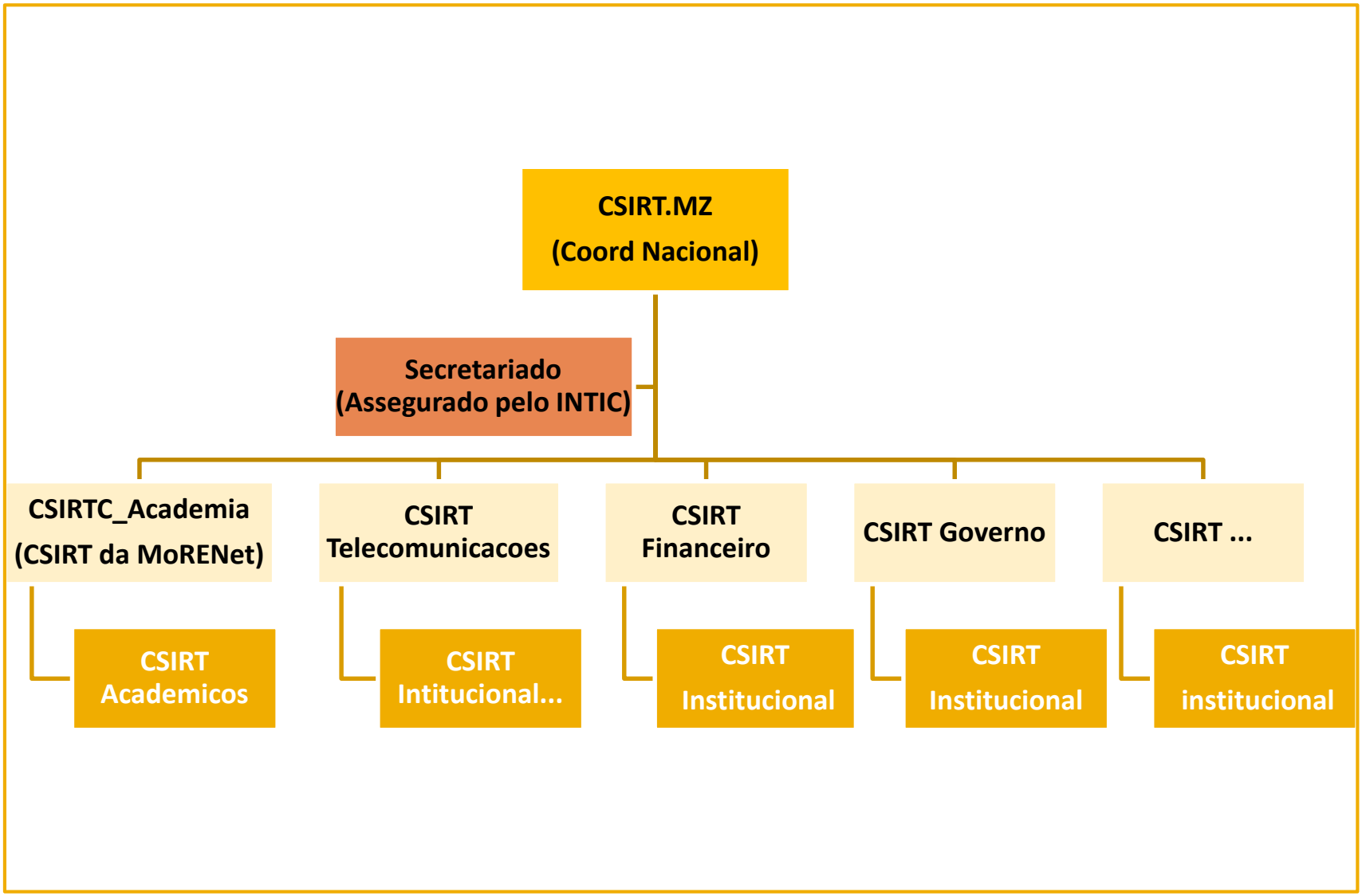
A coordenação da segurança cibernética será assegurada pelo Conselho Nacional de Segurança Cibernética (CNSC).

- uma estrutura de governação a nível político e estratégico
- coordena e lidera as acções que visam a implementação dos objectivos da PENSC.

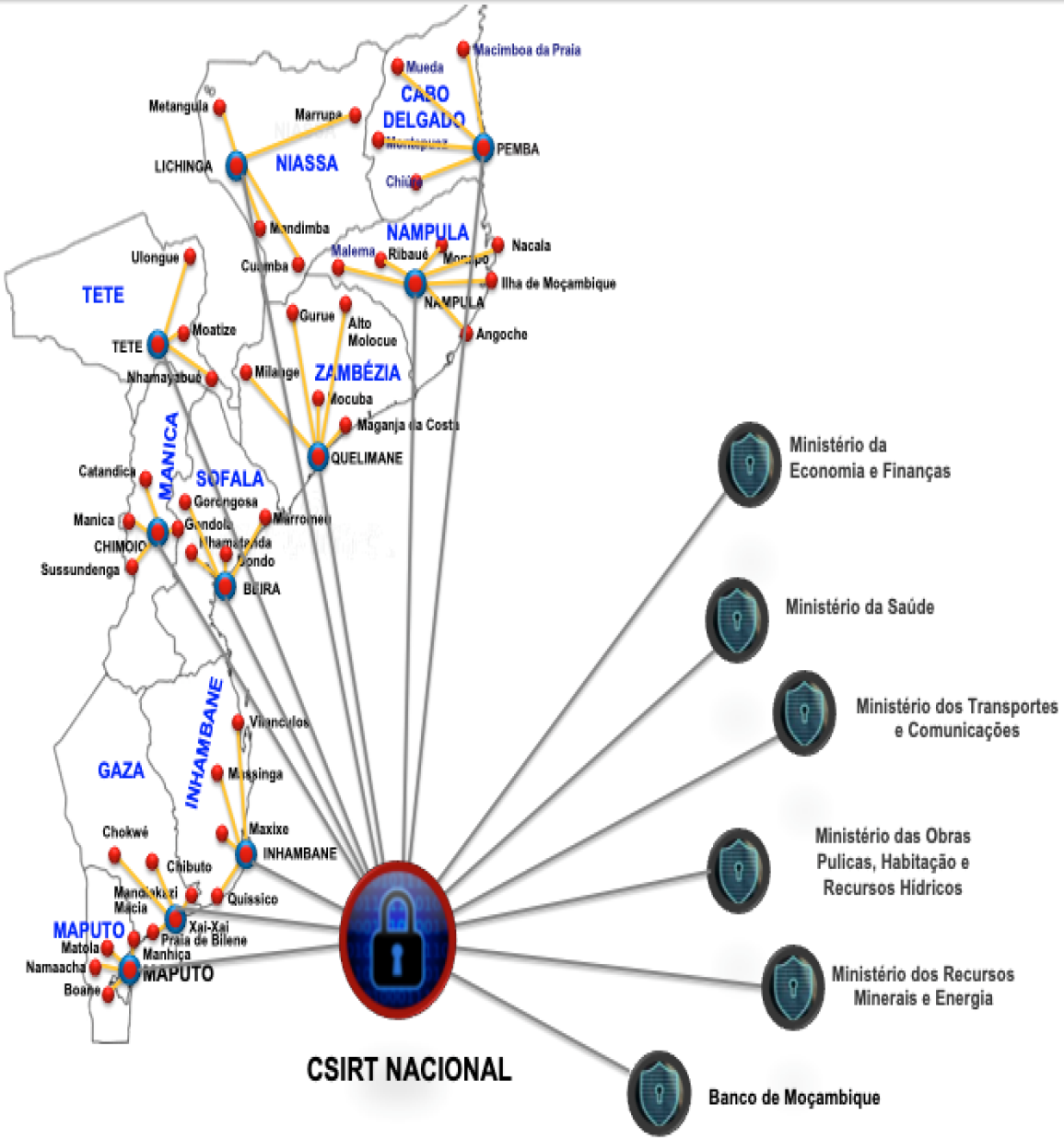


Rede Nacional de CSIRTs

Modelo Hierárquico da Rede Nacional de CSIRT



Rede Nacional de CSIRTs



Rede Nacional de CSIRTs

Abordagem do INTIC no Desenvolvimento da rede nacional de CSIRT

Frameworks e Modelos de Maturidade

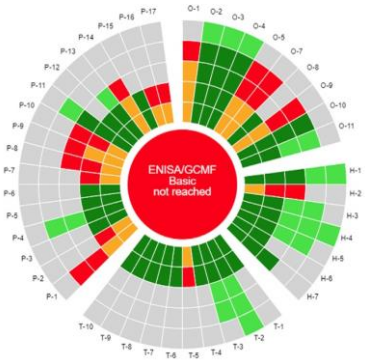
Padrões de Gestão de Incidentes de Segurança Cibernética (Usados no Estabelecimento e Gestão de CSIRTs e SOCs)	
CSIRT Handbook (1998-2003)	ENISA: Guia de Boas Práticas Para Gestão de Incidentes (2010)
FIRST: Framework de serviços CSIRT (v2.1:2019)	ENISA: Como implementar um CSIRT e SOC (2020)
GFCE & NL: Guia para o início do estabelecimento do CSIRT Nacional (2021)	SANS: estabelecimento e gestão de Equipas de Resposta à Incidentes para grandes empresas
ISO/IEC 27035-1&2: Gestão de Incidentes de Segurança da Informação	

Modelo padrão de Níveis de maturidade de CSIRTse

SIM3: Security Incident Management Maturity Model			
Organization	**Human**	**Tools**	**Processes**
• Mandate • Constituency • Authority • Responsibility • Service description • Service level description • Incident classification • Integration in existing CSIRT systems • Organizational framework • Security policy	• Code of conduct/ practice/ethics • Personnel resilience • Skill set description • Internal training • External technical training • External communication training • External networking	• IT resources list • Information sources list • Consolidated e-mail system • Incident tracking system • Resilient phone • Resilient e-mail • Resilient Internet access • Incident prevention tool set • Incident detection tool set • Incident resolution tool set	• Escalation to governance level, Escalation to press function, Escalation to legal function • Incident prevention process • Incident detection process • Incident resolution process • Specific incident process • Audit/feedback process • Emergency reachability process • Best practice e-mail and web presence • Secure information handling process, Information sources process, Outreach process • Reporting process, Statistics process, Meeting process, Peer-to-peer process

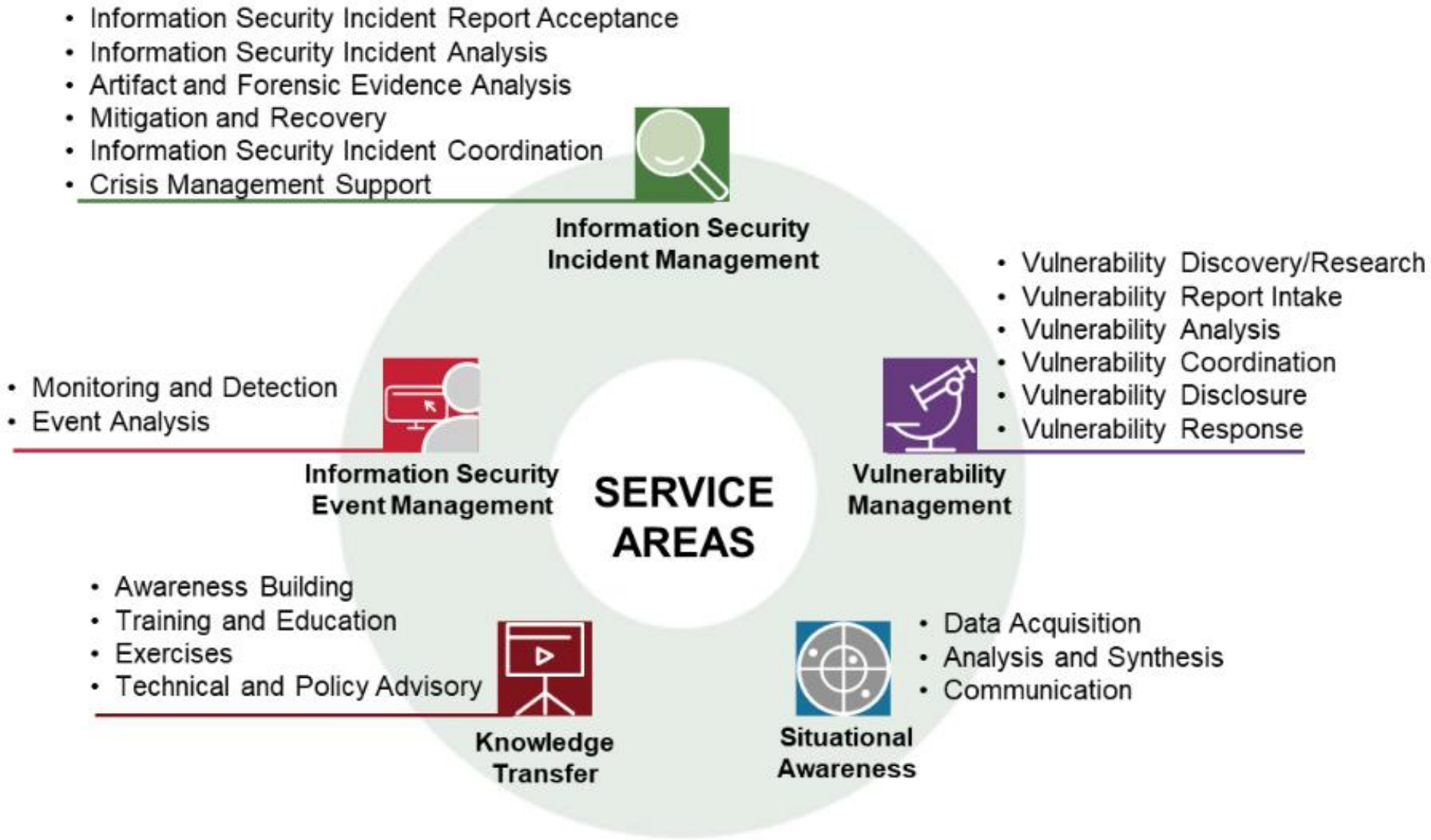
Caracterização do SIM3: 44 Paremtros

1. Organização: 10 Parametros
2. Humanos: 7 Parametros
3. Ferramentas: 10 Parametros
4. Processos: 17 Parametros

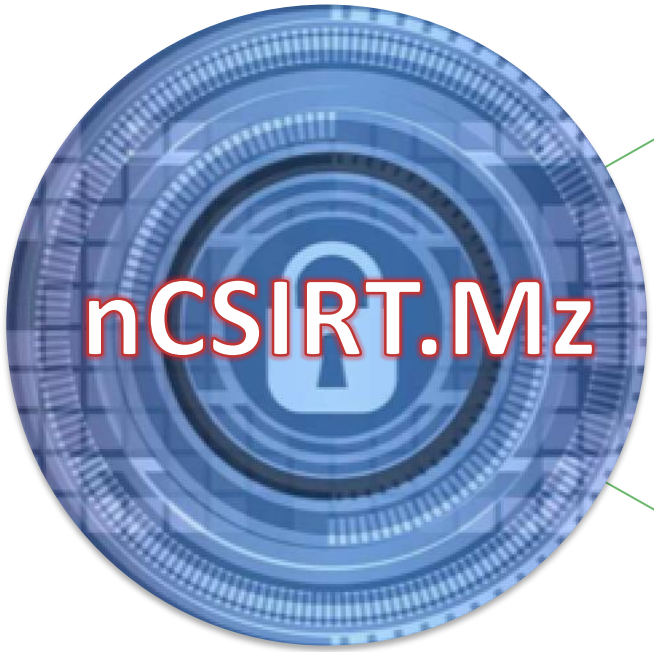


Rede Nacional de CSIRTs

Framework de serviços de um CSIRT (FIRST)



Visão e Missão do CSIRT Nacional (nCSIRT.Mz)



Visão

- Moçambique como uma nação com o espaço cibernético seguro, resiliente e uma sociedade consciencializada.

Missão

- Criar e desenvolver uma capacidade nacional de resposta a incidentes cibernéticos que garanta um ambiente seguro no espaço cibernético Moçambicano em particular e no Ciberespaço Mundial em geral.

CSIRT Nacional

Objectivos da CSIRT Nacional

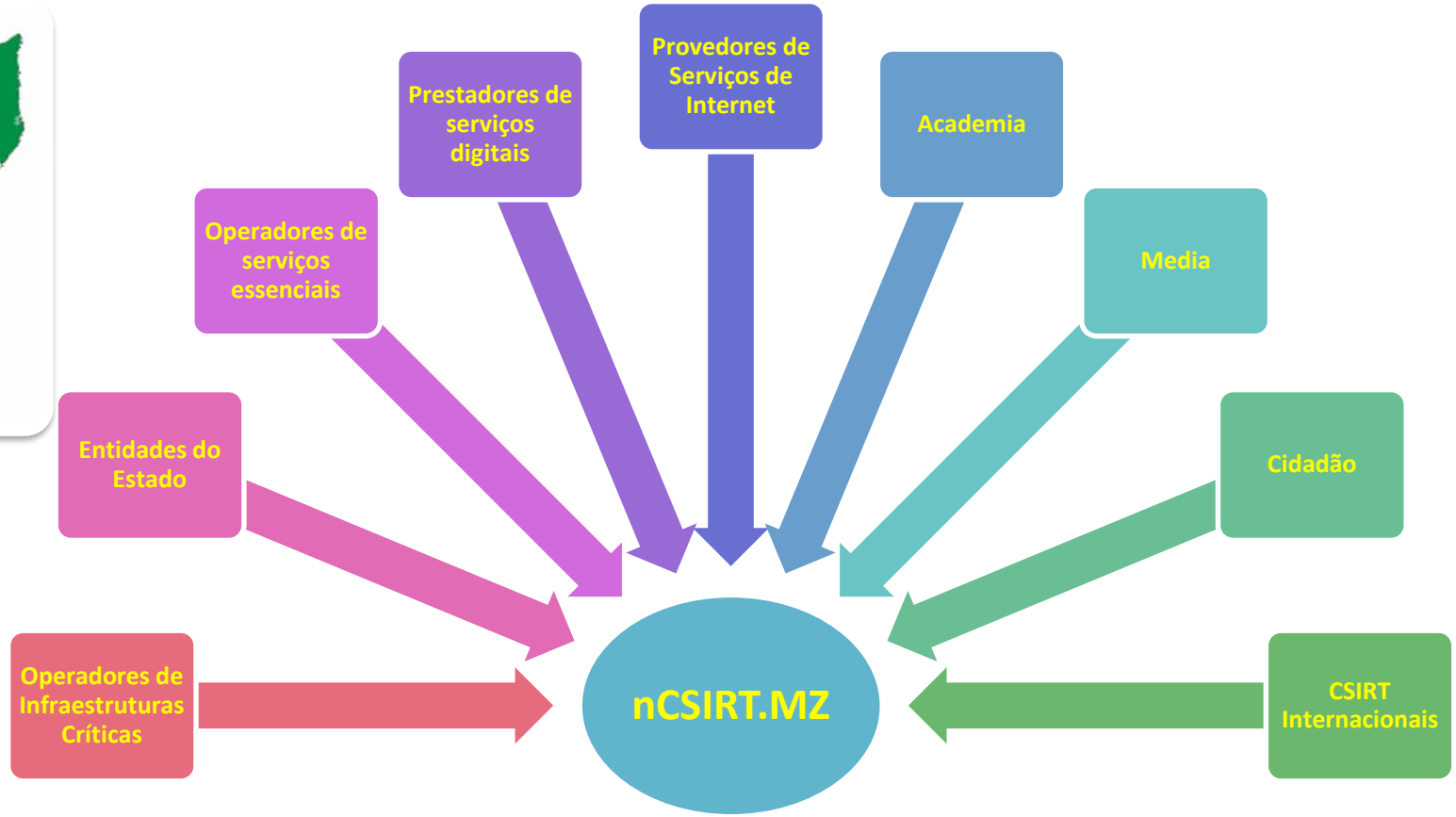
Geral
Estabelecer de uma unidade de coordenação de equipes de resposta a incidentes cibernéticos a nível nacional, que sirva de ponto central de contactos a nível nacional e Internacional.

Específicos

- Coordenar as actividades nacionais no âmbito da operação das equipes de resposta a incidentes;
- Representar o país em fóruns nacionais, regionais e internacionais em matérias de segurança cibernética;
- Dinamizar acções com vista a criação de CSIRTs sectoriais;
- Emanar directrizes, procedimentos, recomendações, normas e padrões técnicos e operacionais, para a melhoria do ambiente de segurança Cibernética;
- Criar e manter o Observatório Nacional de Segurança Cibernética e publicar dados estatísticos sobre a situação de segurança Cibernética no pais;
- Garantir a criação de uma cultura nacional de segurança cibernética.

CSIRT Nacional

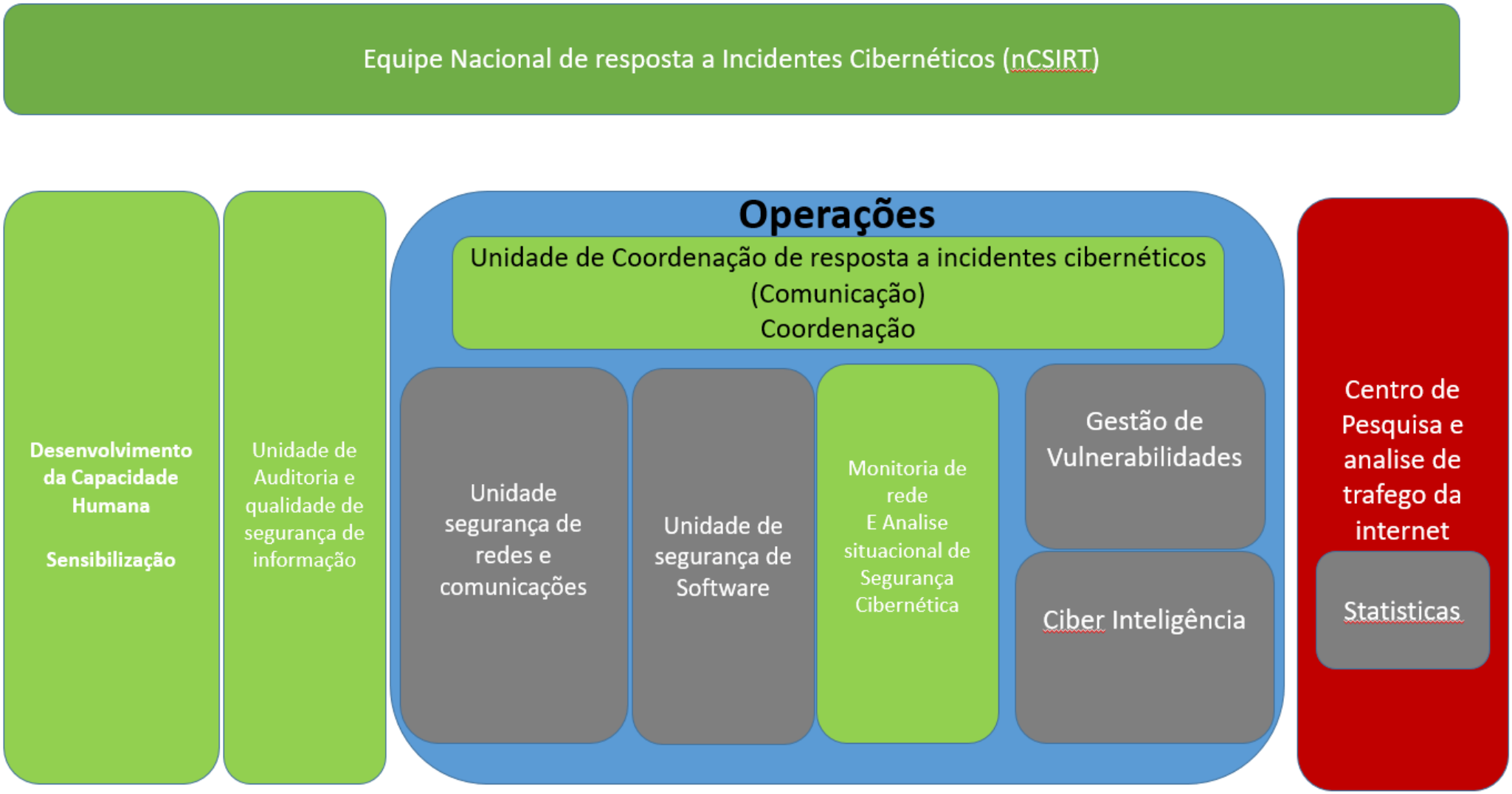
Abrangência (entidades beneficiárias dos serviços do CSIRT Nacional- Conctituency)



De uma forma geral, o ciberespaço de interesse nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações electrónicas, instituição, pessoa coletiva ou singular com sede em território Moçambicano, ou que esteja fisicamente localizado em território Moçambicano

CSIRT Nacional

Áreas funcionais do nCSIRT.Mz



CSIRT Nacional

Serviços actuías do nCSIRT.Mz

Gestão de Incidentes

- Coordenação
- Analise técnica
- Suporte na Mitigação e recuperação

Analise Situacional

- Colecta de dados (HoneyPots Distribuidos, Spampots, Threat feed
- Partilha de informação (MISP)

Transferência de Conhecimento

- Consciencialização
- Desenvolvimento de boas praticas
- Cooperação eventos e reuniões
- Aconselhamento técnico

Público Alvo (Constituency)
Redes que utilizam recursos Nacionais

Principais Atividades

- **Facilitar a coordenação do tratamento de incidentes entre as partes**
- **Auxílio no estabelecimento de novos CSIRTs**
- **Ponto de contato nacional de último recurso**
- **Trabalho colaborativo com outras entidades**
- **Auxílio na análise técnica e compreensão de ataques e ameaças**
- **Aumentar a detecção, correlação de eventos e determinação de tendências**
- **Transferir o conhecimento através de cursos,**
- **Boas práticas e consciencialização**

Fontes de notificação (Feeds)
Membros registados do **ShadowServer**
Abuse.ch
Openfish
Phishtank

Estas atividades vão obedecer o padrão "*FIRST CSIRT Services Framework*", descrito detalhadamente no documento "*Computer Security Incident Response Team (CSIRT) Services Framework*".

CSIRT Nacional

Serviços do nCSIRT.Mz

Página Web do nCSIRT;

(https://csirt.mz)

Sistema de "Ticketing" para registo Incidentes

Um sistema de tratamentos de fontes de informação (feeds) InteMQ e MISP (IoC)

- https://github.com/certtools/intelmq
- https://www.shadowserver.org/

Base de Dados de Contactos

Um Sistema de armazenamento de informação/dados

Tudo o que seja processado pelo IntelMQ deve ficar guardado para:

1)Construção de relatórios e/ou dashboards;

2) Preservação de observáveis referentes ao Ciberespaço Nacional;

RFC-2350

CSIRT Nacional

Cooperação Internacional

O INTIC, IP tem privilegiado a dimensão da cooperação internacional a vários níveis como forma para colher experiências com vista a melhorar o actual cenário no que diz respeito a segurança cibernética.

CSIRT Nacional

Cooperação Internacional (Filiações e acreditações)

- Membros do FIRST
- Membros do AfricaCert
- Membros do "Global Forum Of Cyber Experts"
- Membros dos steering Committee dos CSIRT da SADC

- Cyber4 Dev
- MoU CSA Gana
- MoU NCSA do Ruanda
- MoU CSIR da RSA
- MoU com Eswatini communications commission (esccom)
- Cooperação com o CNCS de Portugal
- Cooperação com CERT.br
- MoU CyberTalents (Osint)

CSIRT Nacional

Oportunidades de Formação - Cooperação com Cybertallent

Pré-requisitos para o curso: http://bit.ly/3YPS1qA
Registo: http://bit.ly/3yGdE27

CSIRT Nacional

Actividades em Curso

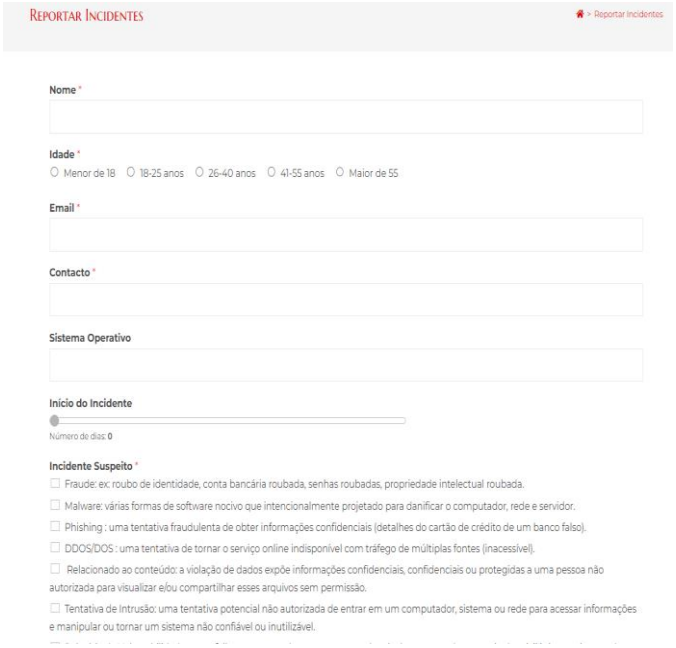
Liderança e Coordenação	• Submetida e em analise a criação do conselho nacional de Segurança Cibernética; • Criado o CSIRT Nacional (Tecnicamente); • Em processo de preparação a criação de um fórum nacional de CSIRTs (Anual);
Protecção de Infraestruturas Criticas	• Em processo de negociação com Gana CSA a cooperação em particular na Matéria de Infraestruturas criticas
Protecção de activos de Informação	• Em processo a Criação da Rede Nacional de CSIRT; • Em carteira o processo de senssibilizacao sobre a necessidade de investimento em segurança Cibernética. • Em analise a adopção de Frameworks sobre segurança para serem adoptados como diretrizes em Moçambique

CSIRT Nacional

Actividades em Curso

Quadro Legal e Regulatório	• Lei de Segurança Cibernética • Lei do Cibercrime e Lei de Protecção de dados • Adesão a convecção de Budapeste
Desenvolvimento de Capacidade, Pesquisa e Inovação	• Assinaturas de MdE: UFSC, UFRGS, Ghana, Ruanda, CSIR, Eswatine para troca de Experiencias; • Em curso a assinatura de um MoU entre o INTIC e Nic.br para disponibilização de cursos online sobre SC; • Criação de uma academia de segurança Cibernética (longo prazo) • Em carteira a criação de curso superiores (Licenciatura e mestrado) de especialização em SC; • Em analise a possibilidade de inclusão de temas ligados a CS no ensino primário e secundário.
Cultura de Segurança Cibernética e Consciencialização	• Em parceria com o CNSC de Portugal foram ministrados cursos de sensibilização para o cidadão no geral e estudantes do ensino secundários em particular • Formação de Jornalistas e actors do ecosistema de SC. • Em curso a assinatura de MoU entre o INTIC e nic.br para disponibilização de cartilhas sobre SC.

Mecanismos de notificação de incidentes



Formulário na pagina do nCSIRT.MZ

https://csirt.mz

E-mail: reportar@csirt.mz

Telefone – Linha verde
800 909 909

Visite a nossa Página

https://csirt.mz

OBRIGADO!!!