INTIC

Instituto Nacional de Tecnologias de Informação e Comunicação

Autoridade Reguladora de TIC

Relatório de Actividades da Equipa Nacional de Resposta a Incidentes Cibernéticos (nCSIRT.mz)

2023 - 2025

MAPUTO

2025

FICHA TÉCNICA

Título: **Relatório de Actividades da Equipa Nacional de Resposta a Incidentes Cibernéticos**

Edição: 1ª Edição

Data de Edição: 02 de Maio de 2025

Classificação: TLP-White

Autor: INTIC, I.P

Equipa de Preparação:

Lourino Chemane, *Presidente do Conselho de Administração do INTIC*
Constantino Sotomane, *Administrador para o Pelouro Técnico Operacional do INTIC*
Eugénio Jeremias, *Director da Divisão de Segurança Cibernética e Protecção de Dados do INTIC*
Ségio Guivala, *Chefe do Departamento de Segurança Cibernética da Divisão de Segurança Cibernética e Protecção de Dados do INTIC e CSIRT Nacional*
Amâncio João Ubisse, *Chefe do Departamento de Estudos, Planificação e Cooperação do INTIC*
Lúcia Zimba, *Técnica do Departamento de Segurança Cibernética da Divisão de Segurança Cibernética e Protecção de Dados do INTIC e CSIRT Nacional*
Elves Teles, *Técnico do Departamento de Segurança Cibernética da Divisão de Segurança Cibernética e Protecção de Dados do INTIC e CSIRT Nacional*

Gráfica:

Amâncio João Ubisse, *Chefe do Departamento de Estudos, Planificação e Cooperação do INTIC*

Av. Rua José Mateus, No. 437, Maputo – Moçambique
E-mail: info@intic.gov.mz, Web: www.intic.gov.mz

RELATÓRIO DE ACTIVIDADES DA EQUIPA NACIONAL DE RESPOSTA A INCIDENTES CIBERNÉTICOS (nCSIRT.mz)

2023-2025

Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC, I.P)

www.intic.gov.mz

MAPUTO

2025

AGRADECIMENTOS

Agradecemos a todas as entidades públicas e privadas nacionais e internacionais que colaboraram connosco ao longo deste período, bem como à nossa equipa técnica, cujo compromisso e profissionalismo foram fundamentais para o cumprimento da nossa missão, sem o qual os resultados aqui apresentados não seriam possíveis.

É de enaltecer a contribuição desses especialistas na criação do nCSIRT.mz, capacitação técnica, participação nas actividades do dia-a-dia, assim como na criação de Equipes de Resposta a Incidentes de Segurança Cibernética Sectoriais e na participação nas missões nacionais e internacionais, como é o caso de exercícios de simulação de incidentes cibernéticos.

Essa contribuição foi fundamental na escolha dos *framework*s adoptados e na definição de métricas concretas para medir o sucesso em todas as fases do processo de operacionalização do CSIRT Nacional e nas diferentes categorias usadas para medir o desempenho de Moçambique em *frameworks* internacionais de medição da segurança cibernética.

ÍNDICE

LISTA DE SIGLAS E ABREVIATURAS

CNSC	Centro Nacional de Cibersegurança de Portugal
CSIRT	*Computer Security Incident Response Team*
FIRST	*Forum of Incident Response and Security Teams*
GCI	*Global Cybersecurity Index*
GFCE	*Global Forum on Cyber Expertise*
ICI	Infra-estruturas Críticas de Informação
IntelMQ	*Intelligence Message Queue*
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
ISP	Provedor de Serviços de Internet
nCSIRT.mz	Equipa de Resposta a Incidentes de Segurança Cibernética Nacional
NIST	*National Institute of Standards and Technology*
NOSi	Núcleo Operacional para a Sociedade de Informação
NU	Nações Unidas
ONSC	Observatório Nacional de Cibe segurança
PADIM	Projecto de Aceleração Digital de Moçambique
PENSC	Política Nacional de Segurança Cibernética e sua Estratégia de Implementação
SIEM	*Security Incident and Event Management*
SIM3	*Security Incident Management Maturity Model*
SR-CSIRT	Equipa Regional de Resposta a Incidentes Informáticos da SADC

LISTA DE FIGURAS E TABELAS

Lista de Figuras

Lista de Tabelas

PREFÁCIO

É com grande satisfação que apresentamos o Relatório de Actividades da Equipa Nacional de Resposta a Incidentes Cibernéticos, documento que reflete os principais esforços, realizações e desafios enfrentados ao longo do período em análise no âmbito da coordenação de acções para a prevenção e mitigação dos efeitos dos incidentes cibernéticos a nível nacional.

Num contexto global cada vez mais digitalizado e interconectado, o reforço da segurança cibernética tornou-se uma prioridade estratégica para os Estados, organizações e cidadãos, sendo que Moçambique não é excepção e encontra-se inserido neste panorama. Através da actuação do CSIRT Nacional, temos procurado responder de forma célere e eficaz às ameaças cibernéticas emergentes, promover a resiliência dos sistemas de informação nacionais e fortalecer a cooperação com parceiros nacionais e internacionais.

Este relatório é parte da concretização do compromisso do INTIC de continuar a trabalhar na operacionalização da Política e da Estratégia Nacional de Segurança Cibernética visando o estabelecimento de um ecossistema nacional de segurança cibernético que concorra para um espaço cibernético mais seguro, inclusivo, resiliente e confiável em Moçambique.

Com este relatório, reforçamos o nosso compromisso de continuar a trabalhar por um espaço cibernético mais seguro, confiável e resiliente.

Maputo aos 02 de Maio de 2025

Prof. Doutor Engº. Lourino Alberto Chemane

Presidente do Conselho de Administração

1 INTRODUÇÃO

No âmbito da implementação da Política Nacional de Segurança Cibernética e sua Estratégia de Implementação (PENSC), aprovado através da Resolução nº. 69/2021, de 31 de Dezembro, foi lançado oficialmente no dia 6 de Abril de 2023, por Sua Excelência Ministro da Ciência, Tecnologia e Ensino Superior, a Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (nCSIRT.mz).

A criação do nCSIRT.mz enquadrava-se no pilar sobre liderança e coordenação da PENSC e tem como objectivo específico, estabelecer um mecanismo nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética.

Com vista a criação e operacionalização do CSIRT Nacional, o Conselho de Administração do INTIC, em 2022, nomeou a Equipa do CSIRT e designou-a as seguintes tarefas:

- Estabelecer uma unidade de coordenação de equipas de resposta a incidentes cibernéticos a nível nacional, que sirva de ponto central de contactos a nível Nacional e Internacional;
- Servir como equipa de resposta de último recurso para incidentes cibernéticos;
- Coordenar as actividades nacionais no âmbito da operação das equipas 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 país; e
- Garantir a criação de uma cultura nacional de segurança cibernética.

As actividades preliminares realizadas pela equipa tiveram como resultado a criação do nCSIRT.mz e da respectiva página web que foi lançada no dia 06 de Abril de 2023 por Sua Excelência Ministro da Ciência, Tecnologia e Ensino Superior.

Desde a sua criação até a presente data, o nCSIRT.mz realizou diversas actividades, como se pode depreender no presente relatório que descreve as actividades realizadas pelo nCSIRT.mz no período compreendido entre Abril de 2023 até Abril de 2025.

1.1 Objectivos

1.1.1 Objectivo Geral

Apresentar as actividades realizadas pela Equipa Nacional de Resposta a Incidentes Cibernéticos (nCSIRT.mz) no período compreendido entre Abril de 2023 e Abril de 2025, avaliando o impacto de suas acções na segurança cibernética nacional e promovendo melhorias contínuas nas práticas de prevenção e resposta aos incidentes cibernéticos.

1.1.2 Objectivos Específicos

1. Descrever as principais acções e operações realizadas pela nCSIRT.mz, destacando o panorama dos incidentes cibernéticos em Moçambique, metodologias aplicadas e as práticas implementadas;
2. Analisar o impacto das acções da Equipe sobre a mitigação de riscos considerando a qualidade das intervenções;
3. Identificar as dificuldades e limitações enfrentadas pela nCSIRT.mz durante o período e propor estratégias para superação desses desafios;
4. Promover a transparência, visando a aumentar a confiança na actuação da equipa;
5. Definir a direcção e prioridades futuras para aprimorar a capacidade de resposta do nCSIRT.mz, alinhando suas actividades com as tendências e necessidades emergentes em segurança cibernética.

1.2 Metodologia

Na elaboração do presente relatório foi adoptada uma metodologia mista**,** de natureza quantitativa e qualitativa**,** para a recolha, tratamento e análise das informações que compõem este relatório. Esta abordagem permitiu uma visão abrangente, não apenas dos números e padrões estatísticos, mas também da complexidade técnica e do contexto operacional na recolha e análise estatística das vulnerabilidades e dos incidentes reportados ao longo do período em análise tendo como base o seguinte:

1. Relatórios das principais actividades realizadas pelo nCSIRT.mz, no período em alusão;
2. Estudo de vulnerabilidades no espaço cibernético nacional;
3. Estudo de dados recolhidos com base na ferramenta IntelMQ;
4. Relatório do Índice Global de Segurança Cibernética (GCI – 2024); e
5. Publicações literárias do nCSIRT.mz.

2 PRINCIPAIS ACTIVIDADES REALIZADAS PELO NCSIRT.MZ

Das diversas actividades que o nCSIRT.mz realizou no período compreendido entre Abril de 2023 a Abril de 2025, destacam-se as seguintes:

2.1 Estabelecimento da Unidade de Coordenação do CSIRT Nacional

No âmbito desta actividade o Conselho de administração do INTIC, IP designou no dia 20 de Junho de 2022 uma equipa de sete (7) técnicos para fazer parte da Unidade de Coordenação do CSIRT Nacional, com função principal de servir de ponto de contacto a nível nacional e internacional, dinamizar o estabelecimento da Rede Nacional de CSIRTs e iniciar com as actividades operativas do CSIRT Nacional.

Do conjunto de actividades realizadas destaca-se as acções de formação aos actores do ecossistema nacional de segurança cibernética, consciencialização pública, cooperação interinstitucional e internacional, desenvolvimento da capacidade operativa para o combate ao crime cibernético, com o objectivo de fortalecer a capacidade da equipa do nCSIRT.mz, para além do estudo de *frameworks* internacionais com destaque aos seguintes: *National Institute of Standards and Technology* (NIST), *Forum of Incident Response and Security Teams* (FIRST) e *Security Incident Management Maturity Model* (SIM3). As secções a seguir apresentam os *frameworks* da FIRST, NIST e SIM3 que têm sido usados na filosofia de actuação do nCSIRT.mz.

2.1.1 Framework de Serviços da FIRST

O Framework de Serviços da FIRST (FIRST CSIRT Services Framework) é uma estrutura de referência desenvolvida pelo *Forum of Incident Response and Security Teams* (FIRST) com o objetivo de padronizar e clarificar os serviços prestados por equipas de resposta a incidentes de segurança informática (CSIRTs). A FIRST é uma organização global que conecta equipas de resposta a incidentes de segurança cibernética e promove a colaboração e a partilha de informações para enfrentar as ameaças cibernéticas de forma mais eficaz.

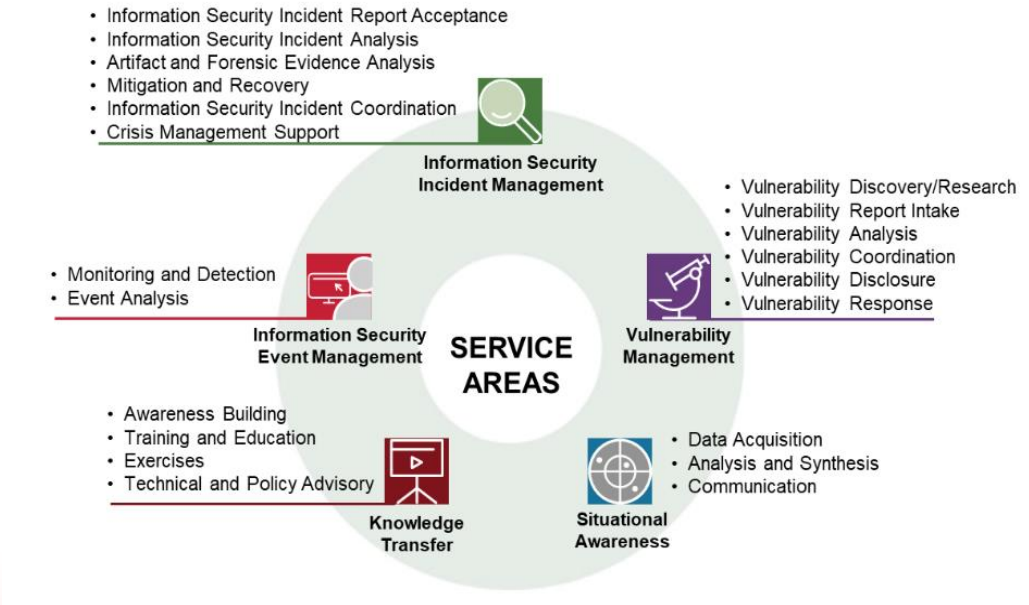

Figura 1: Framework de serviços da FIRST
Fonte: www.first.org

O *framework* de serviços da FIRST, apresentado na figura 1, é voltado para fornecer directrizes operacionais e estratégicas para as CSIRTs, com foco na gestão de incidentes de segurança da cibernéticos. Este *framework* é essencial para coordenar e fortalecer a capacidade global de resposta a incidentes de segurança cibernética e proporciona uma base para que os CSIRTs de diversas partes do mundo possam operar de forma mais padronizada, colaborativa e eficiente, enfrentando desafios de segurança cibernética em escala global.

2.1.2 Framework de Segurança Cibernética da NIST

O Framework de Segurança Cibernética da NIST, (NIST Cybersecurity Framework - NIST CSF) é uma estrutura desenvolvida pelo *National Institute of Standards and Technology* (NIST) dos Estados Unidos, com o objetivo de ajudar organizações de todos os sectores a gerir e reduzir riscos de segurança cibernética. O NIST CSF fornece uma estrutura abrangente que ajuda organizações a identificar, proteger, detetar, responder e recuperar-se de riscos cibernéticos, de forma sistemática, eficaz e alinhada com boas práticas reconhecidas internacionalmente.

O NIST CSF é flexível, permitindo que organizações de qualquer porte ou sector adaptem suas recomendações às necessidades específicas. A figura 2 apresenta as principais componentes do *NIST Cybersecurity Framework*.

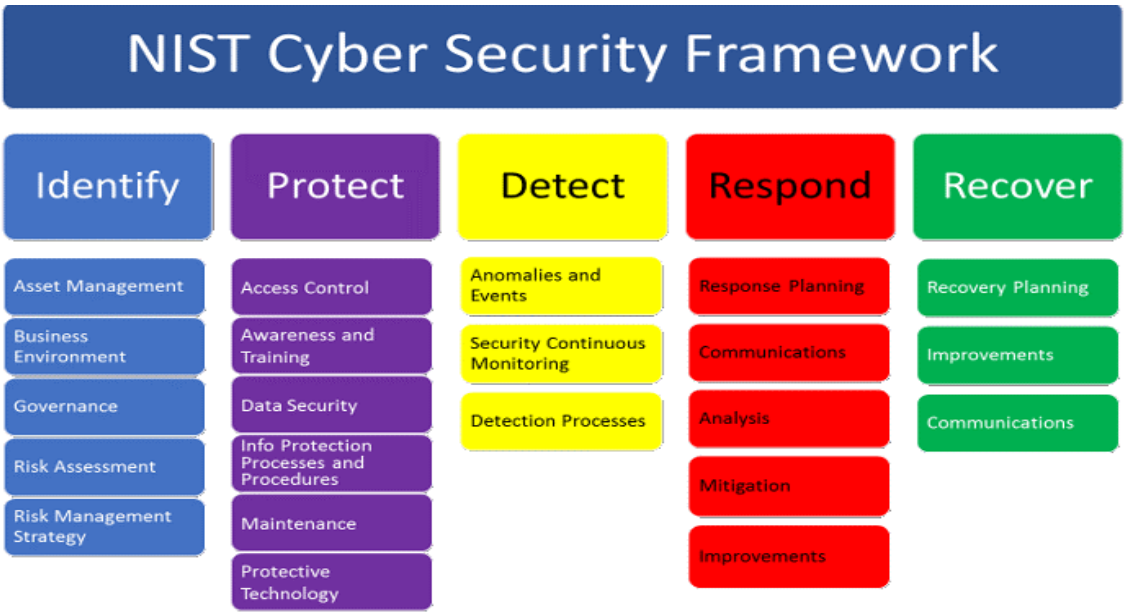

Figura 2: Framework de segurança cibernética do NIST.

Fonte: www.nist.gov

Em 2023 foi lançada a versão 2.0 do *Framework* de Segurança Cibernética (NIST 2.0) que é uma actualização importante do NIST CSF, originalmente lançado em 2014. Esta nova versão reflecte as mudanças nas práticas de Segurança Cibernética, tendo em consideração as ameaças emergentes, novas tecnologias e a evolução do ambiente digital global. O NIST 2.0 continua sendo uma estrutura flexível e adaptável, permitindo que organizações de diferentes tamanhos e sectores realizem a gestão de riscos de segurança cibernética de maneira eficaz.

Na versão 2.0, apresentada na figura 3, o NIST expandiu as funções para incluir mais orientações práticas, especialmente no contexto de governança e gestão de riscos cibernéticos integrados à estratégia de negócios. Isso fortalece a conexão entre a segurança cibernética e a governança organizacional, incentivando que a alta liderança empresarial participe activamente na tomada de decisões sobre a segurança cibernética.

Figura 3: Framework de segurança cibernética do NIST 2.0
Fonte: www.nist.gov

2.2 Identificação de serviços iniciais do CSIRT Nacional

O CSIRT Nacional com base nos *frameworks* apresentados acima, definiu os três primeiros serviços a serem oferecidos que são apresentados de seguida:

- **Gestão de incidentes** - o serviço de gestão de incidentes inclui a análise técnica de ocorrências no espaço cibernético nacional, prevenção e suporte na mitigação de incidentes, incluindo a coordenação da Rede Nacional de CSIRTs;
- **Análise situacional** - este serviço inclui a recolha de dados (através de ferramentas tais como *honeypot* distribuídos, *spampots treat feads*) e partilha de informação através de MISP; e
- **Transferência de conhecimento** - este serviço inclui a consciencialização em vários níveis, desenvolvimento de capacidade técnica, incluído a criação e gestão de CSIRTs, desenvolvimento de boas práticas, desenvolvimento da cooperação, realização de eventos e reuniões de aconselhamento técnico.

Os serviços iniciais prestados pelo nCSIRT.mz são apresentados na figura 4.

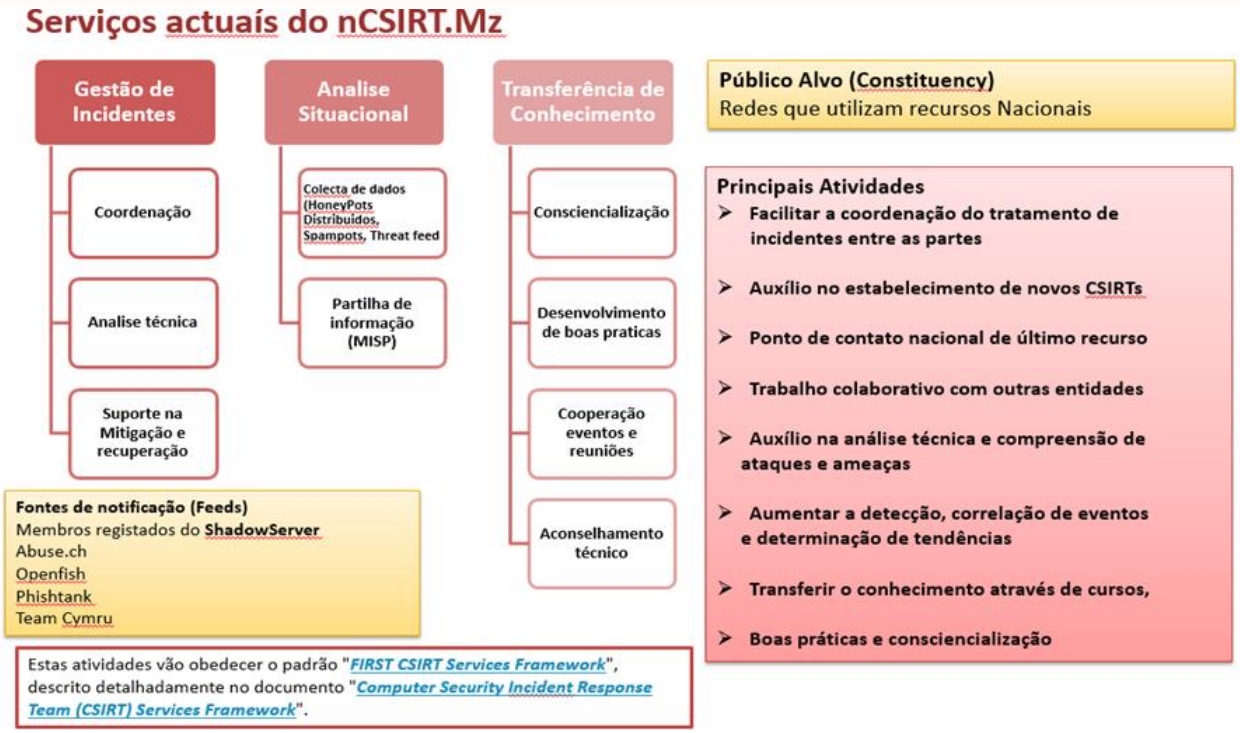

Figura 4: Serviços actuais do nCSIRT.mz.

2.3 Métricas de avaliação do sucesso do nCSIRT.Mz

Um aspecto fundamental no estabelecimento e melhoria dos CSIRT é a definição de métricas concretas para medir o sucesso em suas fases do processo de implementação e acrescimento. O nCSIRT.mz definiu na sua estrutura organizacional as seguintes áreas: (i) Gestão de eventos e incidentes cibernéticos, (ii) Gestão de vulnerabilidades, (iii) Desenvolvimento de capacidade e Transferência de conhecimento, (iv) Análise situacional, (v) Cooperação internacional, e (vi) Desenvolvimento da Rede Nacional de CSIRTs; tendo sido definidas as seguintes métricas para cada categoria:

I. Gestão de eventos de incidentes cibernéticos:
- Número de incidentes detectados;
- Número de incidentes tratados com sucesso (por tipo, origem, automatização, etc.).

II. Gestão de vulnerabilidades:
- Número de verificações de vulnerabilidades realizadas (ou suportadas);
- Número de casos de vulnerabilidade crítica tratados.

III. Desenvolvimento de Capacidade
- Número de quadros capacitados;
- Nº de profissionais com certificações reconhecidas internacionalmente;
- Número de formações realizadas;
- Número de categorias de serviços prestados;
- Número de ferramentas implementadas;
- Número de exercícios de simulação participados.

IV. Análise situacional:

- Número de artefactos CSIRT documentados e disponíveis para análise e partilha;
- Número de fontes de CSIRT que correspondem aos activos constituintes para registo de incidentes;
- Número de recursos partilhados para a consciência situacional (relatórios, alertas, etc.).

V. Cooperação internacional e transferência de conhecimento:

- Número de Memorandos de Entendimentos assinados;
- Número de fóruns, associações ou grupos registados e ou acreditados a nível internacional e nacional;
- Número de Workshops, conferencias, grupos de trabalho participados.

VI. Desenvolvimento da Rede Nacional de CSIRTs:

- Número de CSIRT sectoriais estabelecidos;
- Número de reuniões ou workshops realizados;
- Número de formações realizadas para a criação e gestão de CSIRTs Sectoriais e Institucionais;
- Nº de CSIRTs Sectoriais e Institucionais activos

2.4 Desenvolvimento da página web do nCSIRT.mz

O desenvolvimento da página web do nCSIRT.mz foi uma das tarefas realizadas pela equipa do nCISRT.mz. A página serve como um ponto de contacto permanente com o cidadão e oferece funcionalidades para denúncias através da linha verde, reportes de incidentes através dos formulários, estatísticas sobre incidentes cibernéticos a nível nacional e internacional, cursos de segurança cibernética, manuais de boas práticas e outra informação útil ao cidadão.

A página web do nCSIRT.mz (https://csirt.mz) foi lançada no dia 6 de Abril de 2023 numa cerimónia dirigida por sua Excelência Ministro da Ciência, Tecnologia e Ensino Superior e contou com a presença da Digníssima Procuradora Geral-Adjunta, representantes de CSIRT de África do Sul e Eswatini, quadros do Governo e do INTIC (vide a figura 5).

Figura 5: Momento do lançamento oficial do nCSIRT.mz.

A página web do nCSIRT.mz, ilustrada na figura 6, é um recurso centralizado para promover a segurança cibernética e proteger o cidadão, os activos de informação e Infraestruturas Críticas de Informação, oferecendo suporte técnico, consciencialização pública e educação sobre as melhores práticas de segurança no país.

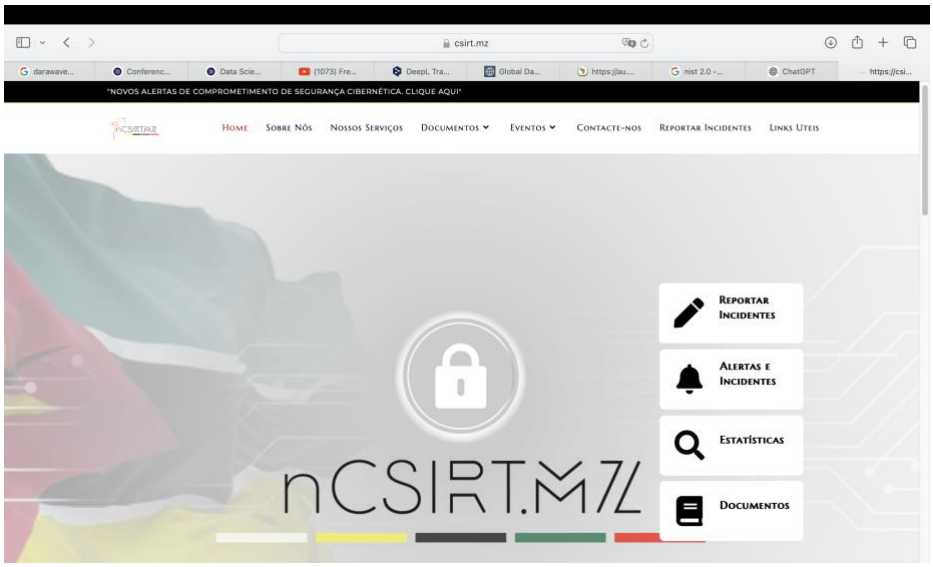

Figura 6: Página web do nCSIRT.mz.

Os principais recursos da página web do nCSIRT.mz são os seguintes:

- **Sobre nós:** Esta secção oferece uma visão geral do nCSIRT.mz, sua missão, visão e objectivos, destacando sua função como órgão central para a coordenação de respostas a incidentes de segurança cibernética em Moçambique.
- **Nossos Serviços:** A secção de serviços oferece uma lista detalhada dos serviços fornecidos pelo nCSIRT.mz, como: monitoramento de ameaças, gestão de incidentes, análise de vulnerabilidades, treinamento e capacitação, relato de incidentes, alertas e notícias.
- **Documentos:** Esta secção reúne arquivos e informações relevantes disponibilizados para a consulta ou *download*.
- **Eventos:** Nesta secção encontram-se informações sobre actividades, encontros e ocasiões especiais organizadas ou promovidas pelo nCSIRT.mz.
- **Contactos:** Inclui informações sobre como entrar em contacto directamente com o nCSIRT.mz, seja via telefone, email ou formulário *online*. Esta secção também inclui informações adicionais sobre como colaborar ou solicitar apoio técnico.
- **Reportar incidentes:** Estão disponíveis três plataformas para reportar incidentes nomeadamente: i) o formulário que pode ser acedido a partir da página do CSIRT

nacional (https://csirt.mz), ii) o e-mail: reportar@csirt.mz e a linha verde, conforme ilustra a figura 7.

- **Links uteis:** Reúne conexões rápidas para páginas, recursos e ferramentas relevantes, tanto dentro quanto fora do site nCSIRT.MZ.

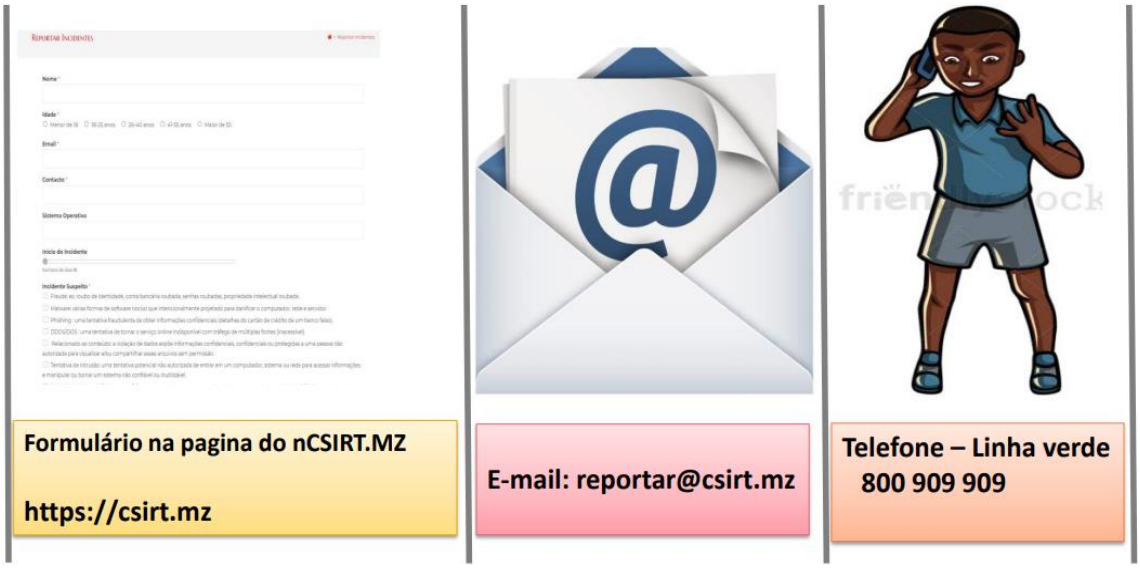

Figura 7: Mecanismo de reporte de incidentes.

Fonte: https://CSIRT.MZ

2.5 Estabelecimento da Rede de Contactos

Durante o período em análise, o nCSIRT.mz através do INTIC, IP estabeleceu Memorandos de Entendimento e acordos de trabalho com várias entidades e Equipas de Resposta a Incidentes de Segurança Cibernética a nível regional e internacional com destaque para AfricaCert, FIRST, INTERPOL, FBI, CERT.PT, Facebook, CSIRT Nacional do Gana, CSIRT Nacional do Ruanda, *Team Cymru*, CNS de Portugal, SEI dos EUA e NIC.br do Brasil.

Figura 8: Assinatura de Memorando de Entendimento com ESCCOM

Figura 9: Assinatura de MoU com Autoridade Nacional de Segurança Cibernética do Ruanda.

A figura 8 ilustra o momento da assinatura de MoU entre INTIC e ESCCOM e a figura 9 ilustra o Presidente do Conselho de Administração do INTIC, Prof. Doutor Eng. Lourino Chemane representando a Autoridade Nacional de Segurança Cibernética de Moçambique e o Presidente da Autoridade Nacional de Segurança Cibernética do Ruanda, o Coronel Davide Kanamugire, momentos depois de assinatura do Memorando de Entendimento.

Os acordos estabelecidos têm sido usados para obter apoio na resolução de incidentes, receber notificações de vulnerabilidades e incidentes referente ao espaço cibernético nacional e obter dados sobre ocorrências de incidentes que são analisados pela equipa do nCSIRT.mz para efeitos de produção de relatórios sobre a segurança cibernética no nosso país. A figura a baixo ilustra momentos da operacionalização do Memorando de Entendimento assinado com o Centro Nacional de Segurança Cibernética de Portugal (CNS de Portugal), onde se destaca o Eng. Lino Santos, Director do CNCS de Portugal reunido com os técnicos do CSIRT Nacional.

Figura 10: Reunião com CNCS para implementação de ferramentas para nCSIRT.mz

Para além dos acordos assinados com instituições congéneres a nível da região e internacional, o nCSIRT.mz é membro de vários fóruns internacional com destaque para: Comité de Direcção da Equipa Regional de Resposta a Incidentes Informáticos da SADC (SR-CSIRT), *Forum of Incident Response and Security Teams* (FIRST), AfricaCert e *The Global Forum on Cyber Expertise* (GFCE).

2.6 Implementação de ferramentas de análise e visualização de ocorrências sobre segurança cibernética

Foram implementadas e configuradas as ferramentas MISP, IntelMQ e Splunk, que de forma integrada permitem alimentar os Sistemas de Gestão de Incidentes e Eventos de Segurança Cibernéticos (Security Incident and Event Management –SIEM) e Bases de Dados que por sua vez fazem correlação de eventos para uma melhor triagem e análise de incidentes. A implementação destas ferramentas permite:

- **Detecção, Triagem e Análise de Incidentes:** A equipa técnica desenvolve acções de detecção, triagem e análise de incidentes cibernéticos. Porém estas actividades devem ser ainda aprimoradas;
- **Detecção de incidentes/Análise da informação recebida:** A equipa do nCSIRT.mz monitora constantemente o espaço cibernético nacional em busca de actividades suspeitas ou anormais, que possam indicar um incidente de segurança cibernética, através da análise das informações colectadas com a ferramenta IntelMQ, e outras fontes de informação;
- **Classificação e triagem:** Classificação da gravidade e prioridade dos incidentes com vista a determinar o nível de resposta necessário e alocar recursos adequadamente;
- **Investigação e análise**: A equipa nCSIRT.mz conduz a investigação para determinar a natureza do incidente, suas origens, o impacto nos sistemas e a extensão do comprometimento;
- **Contenção e mitigação**: Uma vez que o incidente é compreendido, a equipa do nCSIRT.mz toma medidas para conter a propagação do incidente e mitigar seus efeitos dando uma série de recomendações a entidade afectada;
- **Comunicação e coordenação**: Durante todo o processo de resposta a incidentes, a equipa mantém uma comunicação constante com as partes interessadas relevantes, incluindo a gestão executiva, outras equipas, provedores de serviços e, em alguns casos, autoridades legais. A coordenação eficaz é essencial para garantir uma resposta rápida e eficiente;
- **Documentação e relatórios**: Durante todo o processo, a equipa do nCSIRT.mz com o sistema de *Tickets* mantem registos detalhados de todas as etapas tomadas, evidências colectadas e acções executadas. Essas informações são documentadas em relatórios de incidentes que podem ser usados para referência futura, análise forense e treinamento da equipa.
- **Produção de Relatórios:** Com a implementação das ferramentas supracitadas, o nCSIRT.mz produz relatórios trimestrais de forma progressiva, vai melhorando a produção de relatórios sobre incidentes cibernéticos, correlacionar incidentes e alertar sobre tendência e tipos de ataques direccionados ao nosso país como forma de prevenir e remediar incidentes cibernéticos.

2.7 Acções de formação

No âmbito do desenvolvimento de capacidade técnica para o estabelecimento e gestão de CSIRTs e do ecossistema nacional de segurança cibernética, assim como para o desenvolvimento da capacidade técnico-operacional de resposta a incidentes, foram capacitados 2.032 técnicos incluindo jornalistas, tendo sido realizados as acções de capacitação apresentadas tabela 1.

***Tabela 1**: Formações de equipas de CSIRTs*

Período	Formação
Agosto de 2022	Curso Sobre Fundamentos de CSIRT
Outubro de 2022	Curso sobre Modelos de Maturidade de CSIRTs
	Curso Sobre o Relacionamento dos CSIRTs com os Intervenientes Públicos do Ecossistema de Segurança Cibernética
Fevereiro de 2023	Curso Avançado Sobre Gestão de CSIRTs
	Curso Sobre o Relacionamento dos CSIRTs com os Intervenientes Públicos do Ecossistema de Segurança Cibernética
Abril de 2023	Curso Para Criação de Competências Para Formadores
	Curso de Certificação de Auditores SIM3
Julho de 2023	Curso Sobre o Relacionamento dos CSIRTs com os Intervenientes Públicos do Ecossistema de Segurança Cibernética (Tete)
	Curso Sobre Fundamentos de CSIRT (Tete)
	Seminário de Preparação de Exercícios de Incidentes Cibernéticos
Período	**Formação**
Outubro de 2023	Curso sobre Infraestrutura de Segurança do Windows, identificação de ameaças e segurança de *endpoints*
	Gestão e estratégia de risco cibernético
	Curso sobre Protecção da Soberania Nacional através da segurança cibernética
	Curso sobre Privacidade de Dados e Redes Sociais
	Curso sobre Introdução a Protecção da Infraestrutura Crítica Nacional de Informação
	Curso sobre Protecção de Crianças Online
	Curso sobre Tratamento e Resposta a Incidentes de Segurança Cibernética
Outubro de 2023	Cursos online: Cidadão ciberseguro, Cidadão ciberinformado, Consumidor ciberseguro, Cidadão cibersocial em parceria como CNCS de Portugal
Abril de 2025	Modular Higher Education System in Data Protection and Cybersecurity for Supporting the Digital Transformation in Mozambique and South Africa

Os CSIRTs desempenham um papel crucial para a coordenação, colaboração, tratamento de incidentes e consciencialização a vários níveis para a adopção de boas práticas para a redução da exposição aos riscos de segurança cibernética.

No processo de estabelecimento dos CSIRTs em Moçambique que constituem a Rede Nacional de CSIRTs, conforme definido na Política Nacional de Segurança Cibernética e sua Estratégia de Implementação, sendo que durante a sua implementação e operação irá decorrer a auditoria e certificação dos mesmos para segurar que aplicam padrões e apresentam níveis de maturidade aceitáveis e reconhecidos internacionalmente.

As auditorias aos CSIRTs serão realizadas por técnicos nacionais certificados, realçar que Moçambique conta actualmente com 14 (catorze) auditores com certificação SIM3 conferida pela Open CSIRT Foundation (OCF), sendo que 2 (dois) obtiveram a certificação em 2021, enquanto que 12 (doze) foram capacitados em Maputo em 2023. A capacitação destes quadros permitiu ao INTIC iniciar a fiscalização dos CSIRTs Sectoriais e institucionais em implementação no país. A figura abaixo ilustra sessão de atribuição dos certificados dos auditores realizada no MCTES.

Figura 11: Sessão de certificação dos auditores no modelo de SIM3

2.8 Acções de Formação dos Quados do nCSIRT.Mz

A tabela 2 apresenta as formações realizadas para o desenvolvimento de capacidade da nCSIRT.mz no âmbito do Projecto de Aceleração Digital de Moçambique (PADIM)financiado pelo Banco Mundial.

***Tabela 2**: Formação dos quadros no âmbito do PADIM*

#	Formação	No. de Benificiários
1	The Palo Alto Networks Firewall	2
2	Formação em Gestão e segurança de soluções de Hiper Convergência	5
3	Chief Security Information Officer Training	2
4	CheckPoint Firewall Security Administration	3
5	Curso em Privacidade e Protecção de Dados	20
6	ISO 27001 Lead Auditor	8
7	ISO 31000 Lead Risk Manager	2
8	PMBOOK Project Management	3
10	COBIT Certification	4
11	Curso de Desenvolvimento de Competências em Multimídia	1
12	Formação em Plataformas de recolha, tratamento e disseminação de dados estatísticos	4

2.9 Resposta a incidentes cibernéticos

O nCSIRT.mz foi solicitado a responder a incidentes cibernéticos perpetrados contra entidades colectivas e pessoas singulares. Estes incidentes estão relacionados com roubo de identidade, fraudes e *Ransomware*. A tabela 3 apresentam os incidentes reportados, o estágio de resolução e as entidades afectadas.

Tabela 3: *Lista de incidentes reportados*

#	Data	Tipo	Plataforma	Estado	Observação	Entidades afectadas
1	Maio2023	*Ransomware*		Desconhecido		Instituição Privada
2	Junho 2023	Fraude ou roubo de identidade	Rede social (*WhatsApp)*	Resolvido	Encaminhado ao INCM	Instituição privada
3	Setembro 2023	Fraude ou roubo de identidade	Rede social Facebook	Resolvido	Cooperação com Interpol	Cidadão
4	Junho 2024	Fraude ou roubo de identidade	Rede social Facebook (página institucional)	Resolvido	Cooperação com Interpol	Instituição do Governo
5	Agosto 2024	Fraude ou roubo de identidade	Rede social Facebook	Resolvido	Cooperação com Interpol	Cidadão
		injeção de scripts maliciosos e um sitemap.xml	Website	Encaminhado o caso para CSIRT do INAGE	CSIRT do Japão e Moçambique	Instituição do Governo
6	Novembro 2024	Botnet (Servidor malicioso/infectado)	IP address 169.239.104.43	Encaminhado o caso para CSIRT do INAGE	CSIRT do Japão e Moçambique	Instituição do Governo
7	Abril 2025	Fraude ou roubo de identidade	Rede social Facebook (página institucional)	Em curso	Cooperação com Interpol	Instituição do Governo

A figura 12 apresenta graficamente o número e tipo de incidentes reportados no período de 2023-2025, destacando-se abuso de informação (fraude e roubo de identidade).

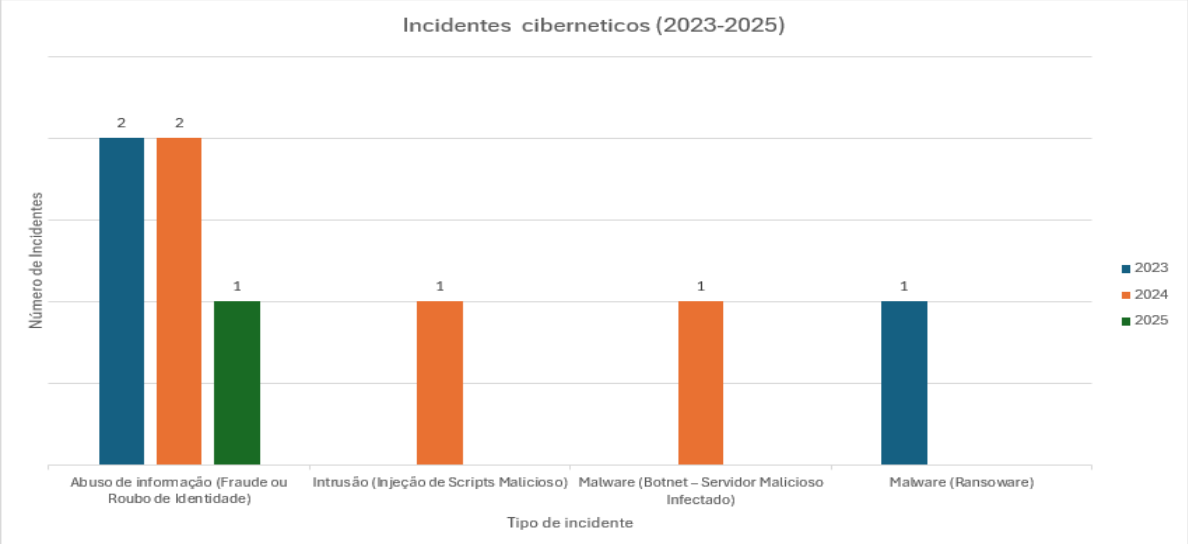

Figura 12:Incidentes cibernéticos

2.10 Acções para o desenvolvimento e fortalecimento de ecossistema nacional de segurança cibernética

No âmbito das acções de coordenação e para o desenvolvimento do ecossistema nacional de segurança cibernética, o nCSIRT.mz realizou vários eventos cujo os principais a destacar os seguintes:

2.10.1 Primeira Reunião Nacional de CSIRTs

Foi realizada no dia 6 de Novembro de 2023 a Primeira Reunião Nacional de CSIRTs, sendo que a sua realização é de periodicidade anual, ficando deste modo estabelecida a plataforma que permite a discussão e análise do grau de implementação e melhorias das medidas de segurança cibernética no país e do estabelecimento da Rede Nacional de CSIRT. A reunião teve a participação de 60 delegados provenientes de todas as províncias do país. A figura 13 ilustra os momentos do decurso da Primeira Reunião Nacional de CSIRTs.

Figura 13: Decurso da Primeira Reunião Nacional de CSIRTs

2.10.2 Workshop sobre Avaliação Nacional de Riscos de Segurança Cibernética com enfoque para as Infra-estruturas Críticas de Informação (ICI)

O *Workshop* sobre Avaliação Nacional de Riscos de Segurança Cibernética com enfoque para as Infra-estruturas Críticas de Informação (ICI) - sob o lema “Moçambique como uma nação com o espaço cibernético seguro e resiliente” foi realizado com o apoio do Governo do Reino Unido. O evento teve como objectivo, realizar a avaliação inicial do risco de segurança cibernética para as Infra-estruturas Críticas Nacionais e melhorar o processo de identificação de infra-estruturas e críticas e serviços essências nacionais para melhor definir políticas e estratégias de protecção das ICI. Como resultado deste workshop foi realizado o levantamento e avaliação do risco das infra-estruturas critica em instituições seleccionadas nesta primeira fase.

2.10.3 Realização do 3º Exercício de Simulação de Incidentes Cibernéticos de África em 2023

O Secretariado da SADC e o *Software Engineering Institute* (SEI) dos Estados Unidos em coordenação com o Ministério da Ciência, Tecnologia e Ensino Superior (MCTES), através do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC, IP) acolheu em Maputo de 07 a 10 de Novembro de 2023, a 3ª Edição da Simulação de Incidentes de Segurança Cibernética de África, denominada "*Africa Cyber Drill 2023*" com o envolvimento do AfricaCERT, o CSIRT Nacional das Maurícias (CERT-UM) e o *Software Engineering Institute* (SEI) dos Estados Unidos da América.

Figura 14: Participantes do Africa Cyberdrill 2023

O Africa Cyber Drill 2023 teve como publico alvo, os CSIRTs Nacionais da SADC, Ministérios, Autoridades Reguladoras, Bancos Centrais, Agências de Implementação de TIC da SADC, Operadores, Agentes de Aplicação da Lei, Procuradorias, Academia e todas as partes interessadas relevantes em lidar com incidentes de segurança cibernética. Este evento contou com a participação de cerca de 100 convidados provenientes de vários cantos do mundo com destaque para representantes dos países da SADC. Importa salientar que, Moçambique participou com 30 delegados sendo 10 provenientes das províncias.

Figura 15: Momentos da cerimónia de abertura e decurso do Africa Cyberdrill 2023

Foram convidadas a participar neste evento, as entidades com a responsabilidade de implementarem os CSIRTs sectoriais, incluindo os CSIRTs provinciais e municipais, como definido na Estratégia Nacional de Segurança Cibernética.

2.10.4 Exercício Internacional de Segurança Cibernética Dedicado ao sector de Energia – Abril 2024

O Exercício Internacional de Segurança Cibernética 2024, dedicado ao Sector da Energia, foi organizado pelo CSIRT Nacional em parceria com o Centro Nacional de Cibersegurança de Portugal (CNSC), Núcleo Operacional para a Sociedade de Informação (NOSi) e Ministério da Economia Digital, ambos de Cabo Verde, no dia 10 de Abril de 2024.

Figura 16: Decurso do Exercício Internacional de Segurança Cibernética 2024.

Figura 17: Momento da realização do Exercício Internacional de Segurança Cibernética 2024.

Com a realização do Exercício Internacional de Segurança Cibernética 2024, dedicado ao Sector da Energia foram obtidos os seguintes resultados:

- Testada a eficácia da coordenação e comunicação entre as partes interessadas, incluindo o regulador, fornecedores de serviços;
- Melhorada a prontidão e os mecanismos de colaboração e comunicação entre as entidades envolvidas no Exercício;
- Avaliada a resiliência e capacidade de recuperação, incluindo testar os planos de contingência, processos de resposta a incidentes e mecanismos de recuperação de incidentes.
- Produzidas as recomendações de aspectos a melhorar no sector de energia do País;
- Melhorada a cooperação internacional e partilhadas informações, melhores práticas e experiências na protecção dos sistemas contra ameaças cibernéticas;
- Desenvolvidas recomendações e melhorias com base nos resultados do exercício, incluindo actualização de políticas, investimentos em tecnologia e infraestrutura, e a implementação de controlos de segurança adicionais.

2.11 Participação em fóruns nacionais e internacionais em matérias de segurança cibernética

O CSIRT Nacional, participa de forma activa em vários fóruns a nível nacional, regional, continental e global em matérias de segurança cibernética com destaque para os seguintes grupos:

2.11.1 Grupo de Trabalho Regional da SADC para criação de Equipes de Resposta a Incidentes Cibernéticos (Regional SR-CSIRT Task Force)

A Equipa Regional de Resposta a Incidentes Informáticos da SADC (SR-CSIRT) é o ponto de contacto da região da SADC que coordena um quadro de colaboração multinacional em questões de segurança cibernética, sendo um mecanismo institucional de coordenação e partilha confiável de informações dos CSIRTs Nacionais e de outras categorias em toda a Região da SADC para criar um ambiente de segurança cibernética mais seguro, mais fiável e colaborativo na Região da SADC.

O SR-CSIRT constitui uma rede (formal e informal) para os CSIRTs da região colaborarem na assistência técnica e jurídica mediante solicitação, e por via dela, estabelecer uma plataforma para capacitação e treinamento para CSIRTs nos estados membros. O SR-CSIRT servirá também como ponto de contacto para recursos regionais e internacionais que podem prover ajuda em questões temáticas de segurança cibernética que afectam a região.

Moçambique através do nCSIRT.mz é membro efectivo do Comité de Direcção deste grupo de trabalho da SADC.

2.11.2 Rede Africana de Autoridades de Segurança Cibernética (ANCA)

A *Smart Africa* é um compromisso ousado e inovador dos Chefes de Estado e de Governo africanos para acelerar o desenvolvimento socioeconómico sustentável no continente, conduzindo África para uma economia do conhecimento através do acesso acessível à banda larga e à utilização de tecnologias de informação e comunicação.

A Rede Africana de Autoridades de Cibersegurança (ANCA) é parte do projecto *Smart Africa* e é um sub-órgão que reúne várias autoridades e agências africanas de segurança cibernética de diferentes regiões para estabelecer uma plataforma de colaboração e melhorar a coordenação da segurança cibernética em África. A ANCA pretende se tornar um trampolim para ideias e facilitar o reforço da harmonização, coordenação e aprendizagem entre países com suas estratégias de segurança cibernética e entre as partes interessadas, bem como organizar uma cooperação estreita entre os seus membros, ao mesmo tempo que faz ouvir a voz de África nas suas negociações com parceiros de todo o mundo em questões de segurança cibernética.

Moçambique através do INTIC participa das várias reuniões deste grupo tendo participado recentemente na terceira e quarta reunião deste órgão realizadas em Marrocos em 2024.

2.11.3 Fórum Global sobre Especialização Segurança Cibernética (GFCE)

O *Global Forum on Cyber Expertise* (GFCE)" é uma comunidade composta por múltiplas partes interessadas, com mais de 200 membros e parceiros incluindo governos, organizações internacionais, empresas e acadêmicos de todas as regiões do mundo. O GFCE é a plataforma para cooperação internacional no fortalecimento da capacidade e expertise cibernética globalmente.

O INTIC através do nCSIRT.Mz e membro do GFCE e tem participado de forma activa nas reuniões deste grupo fazendo parte de vários grupos específicos de interesse onde tem colaborado. O nCSIRT.Mz participou na Reunião Global do GFCE que decorreu de 10 a 11 de Setembro de 2024 na sede da Organização dos Estados Americanos (OEA) em Washington D.C. e participou virtualmente da Reunião Africana do GFCE realizada em Adis Abeba tendo participado num dos painéis como orador.

2.11.4 Forum of Incident Response and Security Teams

O *Forum of Incident Response and Security Teams* (FIRST) é uma confederação internacional de equipes confiáveis de resposta a incidentes informáticos que lidam cooperativamente com incidentes de segurança informática e promovem programas de prevenção de incidentes.

O FIRST visa promover a cooperação e a coordenação na prevenção de incidentes, estimular a reação rápida aos incidentes e promover a partilha de informações entre os membros e a comunidade em geral. A associação é composta por mais de 600 equipes com representação de mais de 100 nações.

O INTIC através do nCSIRT.mz, faz parte do programa "*fellowship*" do *Forum of Incident Response and Security Teams* (FIRST) e tem beneficiado de financiamento para participar nas diversas conferências, formações, *webnars* e grupos de trabalhos. Como membros do programa fellowship, beneficiamos também de acesso a uma rede de especialistas em segurança cibernética.

2.11.5 Participação na Cimeira Africana de Segurança Cibernética

Sob o lema "**Artificial Intelligence and Trusted Cloud: A Pillar for Strengthening Cybersecurity,"** (Inteligência Artificial e Nuvem Confiável: Um Pilar para o Fortalecimento da Segurança Cibernética), o nCSIRT.Mz fez-se representar neste fórum realizado de 3 a 5 de Fevereiro de 2025 em Rabat, Marrocos sendo que esta edição reuniu ministros, altos funcionários do governo, renomados especialistas internacionais e líderes do sector privado. De forma colaborativa foram exploradas questões estratégicas relacionadas com a transformação digital e a segurança do ciberespaço em África, ao mesmo tempo que partilharam soluções inovadoras para enfrentar os desafios actuais e futuros.

Figura 18: Momentos da Cimeira Africana de Segurança cibernética

2.11.6 Reunião de Alto Nível sobre Inteligência Artificial para África:

O nCSIRT igualmente acompanhado pelo Presidente do conselho de Administração do INTIC, participou da Reunião de Alto Nível Sobre Inteligência Artificial para África, organizado pelo *Smart Africa*, num movimento histórico para posicionar África como um líder estratégico na economia global de Inteligência Artificial (IA), a *Smart Africa* recomendou a criação do Conselho Africano de IA para criar um plano de acção que responda à oportunidade urgente como forma de aproveitar a IA para a competitividade e o crescimento inclusivo de África através da colaboração, investimento e exportações transfronteiriças.

O nCSIRT participou em vários grupos de trabalhos que produziram um conjunto de recomendações estratégicas incluídas na "Declaração de África sobre Inteligência Artificial", apresentada na declaração oficial na Cimeira Global de IA em África, realizada de 3 a 4 de Abril de 2025. em Kigali, Ruanda.

Figura 19: Cimeira Global de IA em África

O anúncio da Declaração da África sobre Inteligência Artificial, mereceu maior atenção no momento inaugural da IA Global sobre a África, marcando o ponto mais alto da transição crucial para a jornada da IA da África. A declaração procura: a) Aproveitar o potencial da IA para impulsionar a inovação e a competitividade para promover as economias, indústrias e sociedades da África; b) Posicionar a África como líder global em adopção da ética, confiável e inclusiva da IA; e b) Promover o design, desenvolvimento, implantação, uso e governança sustentáveis e responsáveis das tecnologias de IA em África.

A tabela 4 apresenta a lista de eventos nacionais e internacionais que o nCSIRT.mz participou no período em referência.

***Tabela 4**: Lista de eventos nacionais e internacionais do nCSIRT.mz*

#	Local	Tipo	Evento	Data	Financiador
1	Remoto	Conferência	C-DAYS	14 a 16 de Junho de 2023	
2	Malawi	CyberDrills	11ª edição da ITU CyberDrills da Região Africana.	8 a 12 de Maio de 2023	Cyber4Dev
3	*Online*	Formação	Introduction to Cybersecurity Bootcamp 2023 da Cyber talents	4 a 27 de Junho de 2023	*CyberTalents*
4	*Online*	CyberDrills	APCERTDRILl	16 de Agosto de 2023	
5	Lusaka-Zâmbia	Workshop	Workshop Regional sobre o Combate ao Cibercrime	14 a 17 de Agosto de 2023	
6	Maurícias	Workshop	ECOWAS Regional CSIRT/LEA Inter-agency Co-operation Exercise	26 a 29 de Setembro de 2023	Projecto *Gracy+* do Conselho da Europa
7	Abu Dhabi	CyberDrills	11th Regional Arab, OIC-CERT & CIS Cyber Drill and the Arab Regional Cybersecurity Week	09 a 13 de Outubro 2023	
8	Rabat, Marrocos	Reunião	Terceira reunião da ANCA	08 de Fevereiro de 2024	Smart Africa e Governo do Marrocos
9	Marakesh-Marrakesh	Reunião	Quarta reunião da ANCA	28 de Maio de 2024	Smart Africa e Governo do Marrocos
10	Fukuoka-Japao	Conferência	Quarta reunião anual do FIRST	09-15 de Junho 2024	FIRST
11	Washigton DC	Conferência	Reunião anual do GFCE	10 e 11 de Setembro de 2024	GFCE
12	Nairobi - Quénia	Formação	*SEI Cybersecurity Incident Response Training - Kenya 2024*	22 – 24 de Outubro de 2024	SEI Carnegie Mellon University
13	Abu Dhabi – EAU	Conferência	CyberQ Conference	12 e 13 de Novembro de 2024	ITU
14	Lisboa	Formação	*Chief Security Information officer training (CCISO)*	25 a 30 de Novembro 2024	PADIM
15	Livingstone-Zambia	Simpósio	a 2024 FIRST & AfricaCERT Symposium: Africa and Arab Regions	25 a 29 de Novembro de 2024.	FIRST/AfricaCert

3 ANÁLISE DE VULNERABILIDADES NO ESPAÇO CIBERNÉTICO NACIONAL-2024

O CSIRT Nacional tem recolhido informações de inteligência de ameaças cibernéticas usando meios próprios e também obtém dados a partir dos parceiros com acordos de cooperação firmados. A partir destes dados são realizadas análises de ocorrências e vulnerabilidades a ataques cibernéticos em Moçambique. Algumas destas análises são apresentadas na secção a seguir.

***Tabela 5**: Dados do nCSIRT em 2024*

#	Descrição de dados	Descrição de atributos
1	Tipo de Ocorrência	Bot, Brute force, Darknet, Honeypot, Openresolver, Proxy e Scanner
2	IP	Vários IPs
3	ASN	Vários ASNs
4	Portas de ocorrência	22, 23, 53, 80, 81, 445, 1433, 2222, 2323, 6881, 8080, 37215
5	Data de ocorrência	18 Março a de 31 Dezembro de 2024
6	Hora de ocorrência	24 horas
7	Provedor	15 ISP's que operam no território Nacional

Por razões de privacidade, ao longo do relatório os dados serão anonimizados e representados aleatoriamente e Provedores de Serviços de Internet serão designados por Provedor 1, Provedor 2, …, Provedor 15.

Ao longo de relatórios chamaremos de ocorrências em vez de ataques porque o nCSIRT.mz está ainda a trabalhar com as entidades e provedores que são alvos destas ocorrências para determinar a efectividade dos mesmos.

***Tabela 6:** Ocorrência no espaço cibernético nacional no período de Abril a Dezembro de 2024*

Count of Ocorrências	Column Labels										
	⊞Mar	⊞Apr	⊞May	⊞Jun	⊞Jul	⊞Aug	⊞Sep	⊞Oct	⊞Nov	⊞Dec	Ocorrências Total
Row Labels											
bot	297	898	608	871	406	1	39	4415			7535
bruteforce	39		3	22	137	99	34	193	195	65	787
darknet	6469	13925	16927	15063	18868	15930	15399	32922	20633	8829	164965
honeypot	16	18	14	14	71	6	10	26	2	12	189
openresolvers	1						1				2
proxy	1	11	2	3							17
scanner	5	9	19	19	25	17	23	80	66	12	275
Ocorrências Total	**6828**	**14861**	**17573**	**15992**	**19507**	**16053**	**15506**	**37636**	**20896**	**8918**	**173770**

Da análise realizada, constatou-se que, no período em referência, o espaço cibernético nacional registou um total de 173.770 ocorrências, sendo o maior número de ocorrências relacionado com *Darknet* com 164.965 casos, seguido de *Bot* com 7.535 casos. O tipo de ocorrências menos frequente foi *Openresolver* com apenas 2 ocorrência (quase 0%), desde 18 de Março de 2024. O mês de Outubro foi o que mais ocorrências registou com um total de 37.636 ocorrências. A informação sobre as ocorrências no período em análise é apresentada na figura 20.

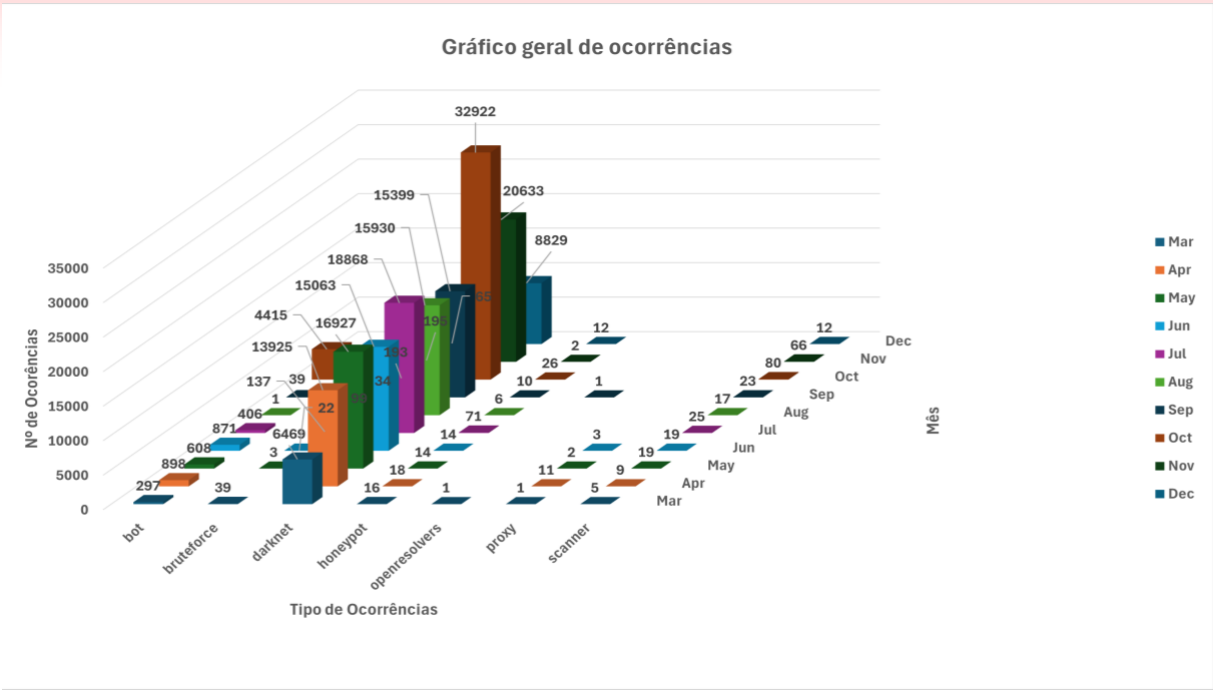

Figura 20: Número de ocorrências a nível nacional (2024)

O gráfico abaixo mostra as portas que são alvo das ocorrências registradas, com destaque da porta 445 (TCP- *Server Message Block*) com 59.808 ocorrências que corresponde a 34,0%, porta 1433 (TCP-*Mysql Server*) com 54.555 ocorrências que corresponde a 31% e porta 23 (TCP-*Telnet*) com 40508 ocorrências que corresponde a 23,0%.

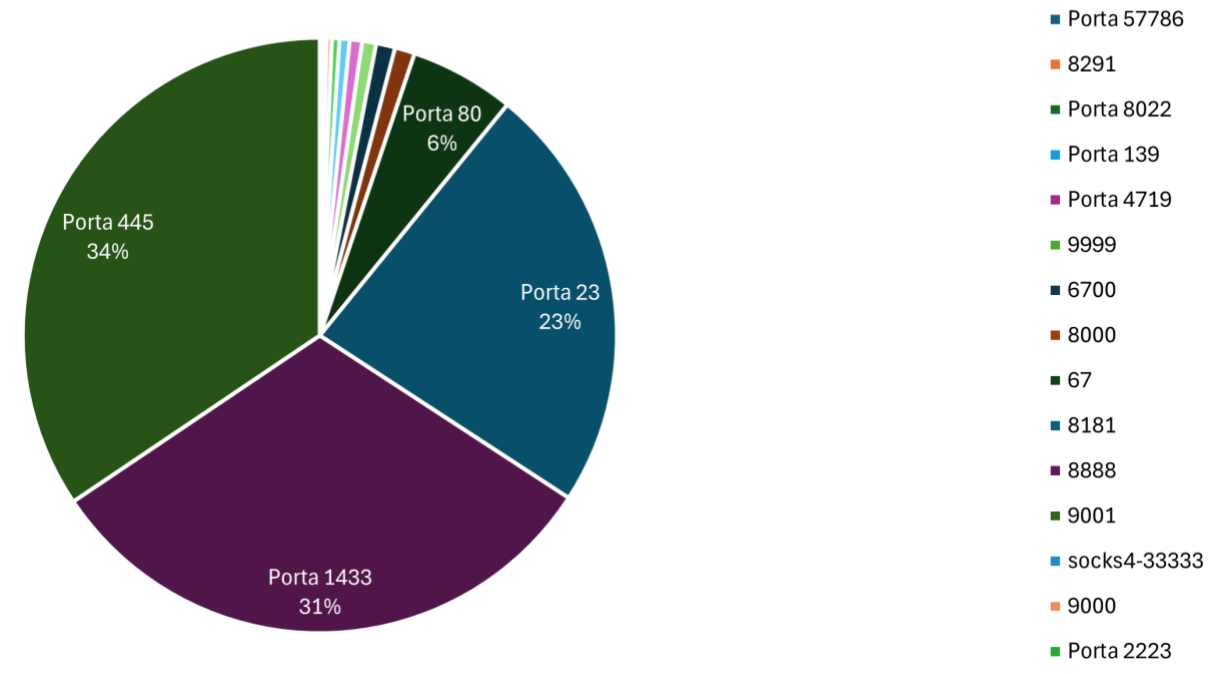

Figura 21: Número de ocorrências por portas *(2024)*.

O gráfico abaixo, apresenta o número de ocorrências por provedor. Como foi referido anteriormente, por razões de privacidade os provedores foram anonimizados e são designações por Provedor 1 a Provedor 15. No gráfico, nota-se que o Provedor 12 e o Provedor 13 registaram maiores ocorrências com 43.015 que corresponde a 24,7% e 103.495 que corresponde a 59,5%, respectivamente. A maior parte de ocorrências registadas nos provedores são de IPs relacionados a actividades na *Darknet*.

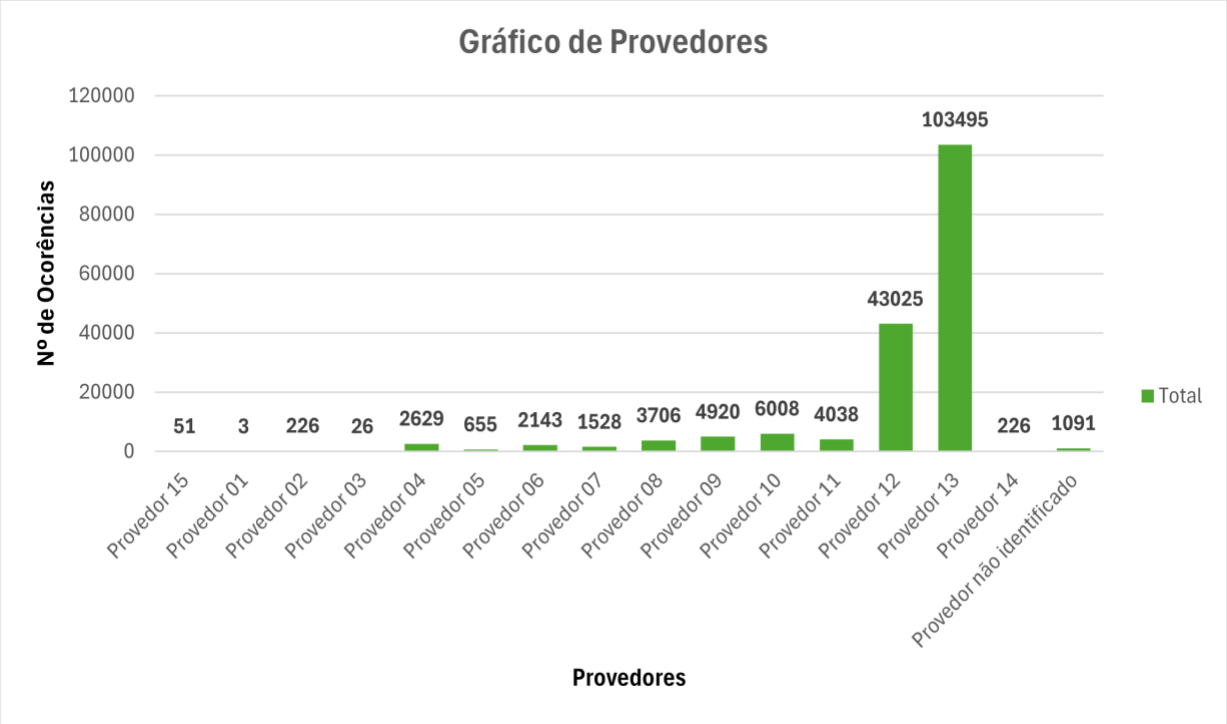

Figura 22: Número de ocorrências por provedores (2024).

O gráfico abaixo representa o período, em que foram registadas as ocorrências. Durante o período em análise, constatou-se que o pico de registo das ocorrências é no intervalo das 00:00H (12:00 AM) às 1:00H (01:00 AM) com destaque a Darknet com 164.965 ocorrências.

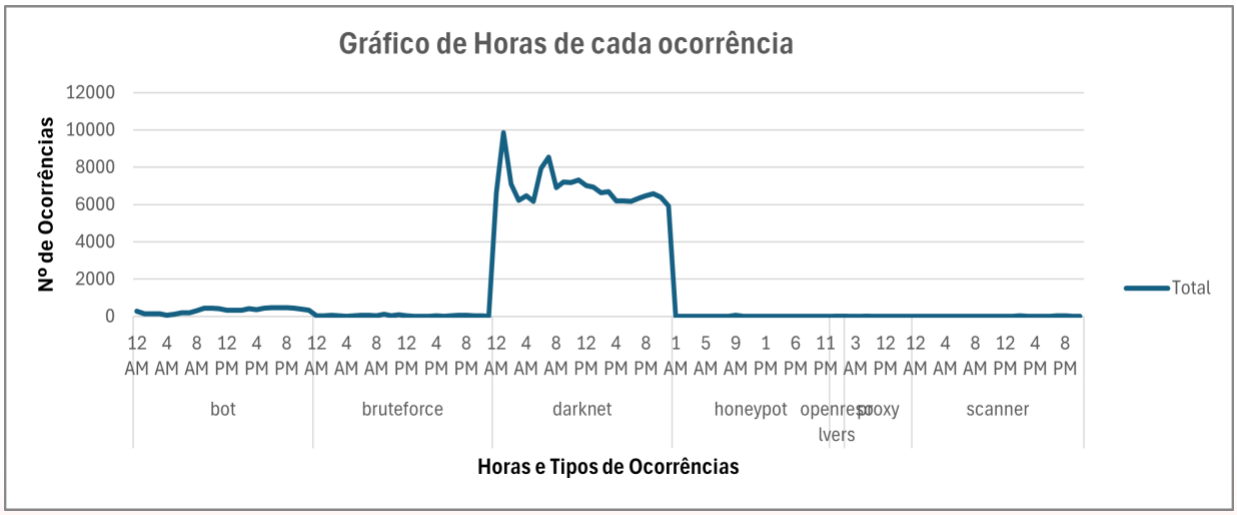

Figura 23: Tempo de registo das ocorrências (2024).

Para além dos dados acima apresentados, foram implementados mecanismos de recolha de dados estatísticos que vão alimentar o Observatório Nacional de Segurança Cibernética recentemente estabelecido e a emissão de vários relatórios sobre segurança cibernética no país.

Tabela 7: *Ameaças no espaço cibernético nacional no período de março a julho de 2023.*

#	Vulnerabilidades	Nº de Ocorrências	Percentagem
1	Acessible-http	12764	3.4%
2	Acessible-msrdp-udp	21	0.0%
3	Blacklisted-ip	20510	5.4%
4	Dns-open-resolver	31	0.0%
5	Open-like	888	0.2%
6	Open-rdp	27391	7.2%
7	Open-ssl	311588	82.2%
8	Open-vnc	3124	0.8%
9	Spam-url	1	0.0%
10	Vulnerable-exchange-server	2465	0.7%
11	Vulnerable-smtp	108	0.0%
12	**Total**	**378891**	**100.0%**

4 ANÁLISE DE VULNERABILIDADES NO ESPAÇO CIBERNÉTICO NACIONAL - 2025

Como referido anteriormente por razões de privacidade, ao longo do relatório os dados serão anonimizados e representados aleatoriamente e Provedores de Serviços de Internet (ISP) que serão designados por Provedor.

Ao longo de relatórios chamaremos de ocorrências em vez de ataques porque o nCSIRT.mz está ainda a trabalhar com as entidades e provedores que são alvos destas ocorrências para determinar a efectividade dos mesmos

Tabela 8: *Dados do nCSIRT em 2025*

#	Descrição de dados	Descrição de atributos
1	Tipo de Ocorrência	Brute force, Darknet, Honeypot,e Scanner
2	IP	Vários IPs
3	ASN	Vários ASNs
4	Portas de ocorrência	22, 23, 53, 80, 81, 445, 1433, 2222, 2323, 6881, 8080, 5555,8,26,386,8889,6962,60023,10023,4719,10443,30003,58443,60009,9999,2601,7777,2332
5	Data de ocorrência	Janeiro - Março de 2025
6	Hora de ocorrência	24 horas
7	Provedor	9 ISP's que operam no território Nacional

Da análise realizada, constatou-se que, no período em referência, o espaço cibernético nacional registou um total de 36330 ocorrências, sendo o maior número de ocorrências relacionado com *Darknet* com 36118 casos, correspondendo a 99.4%, seguido de *honeypot* com 55 casos, bruteforce com 54 casos. O tipo de ocorrências menos frequente foi o scanner com 38 casos ocorrência (quase 0%), como é apresentada na figura 24.

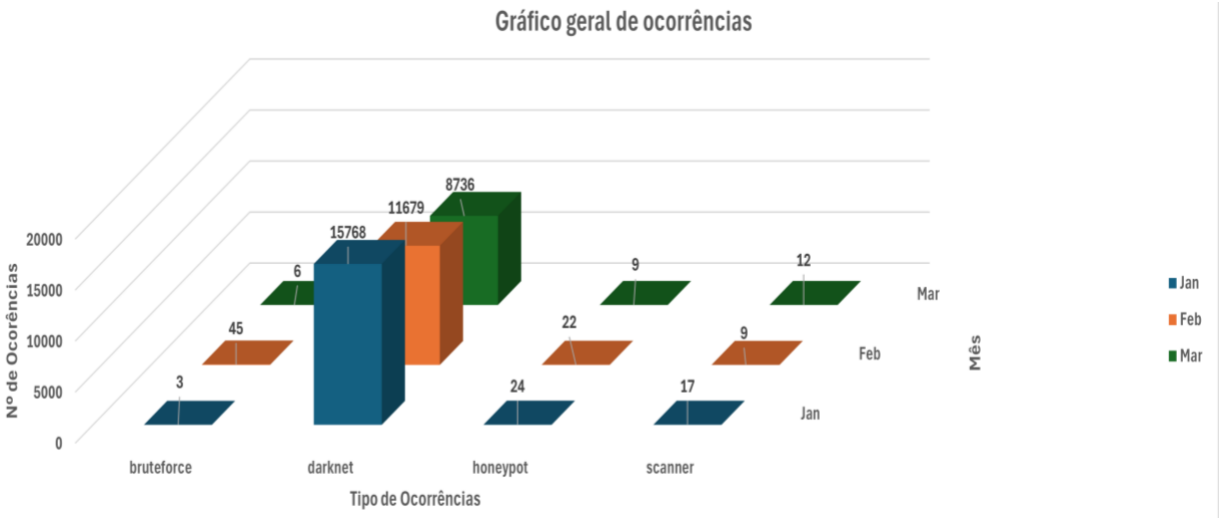

Figura 24: Número de ocorrências a nível nacional (2025)

O gráfico abaixo mostra as portas que são alvo das ocorrências registadas, com destaque da porta 445 (TCP- *Server Message Block*) com 11.744 ocorrências que corresponde a 32,0%, porta 1433 (TCP-*Mysql Server*) com 11794 ocorrências que corresponde também a 32,0% e porta 23 (TCP- *Telnet*) com 11098 ocorrências que corresponde a 31,0%.

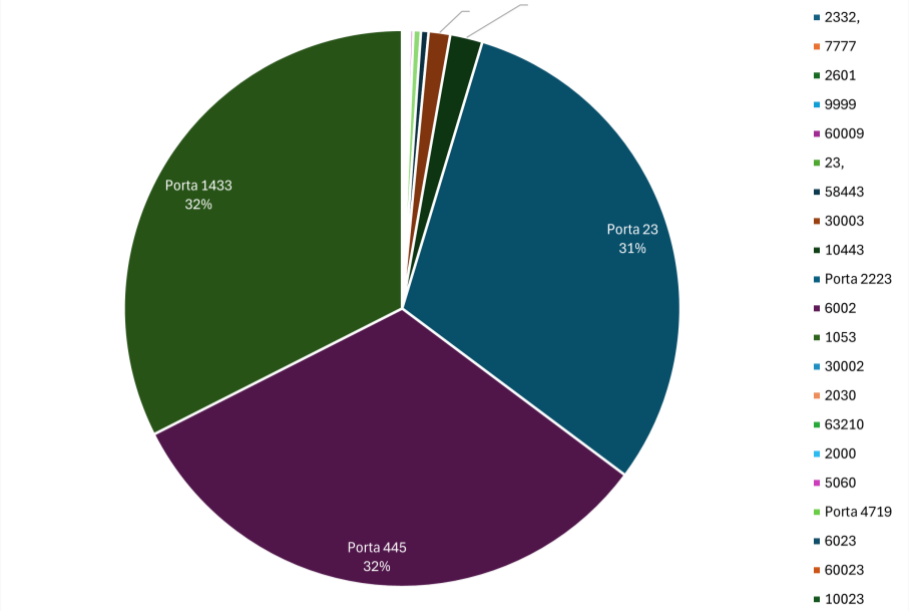

Figura 25: Número de ocorrências por porta (2025)

O gráfico abaixo, apresenta o número de ocorrências por provedor. Como foi referido anteriormente, por razões de privacidade os provedores foram anonimizados e são designações por Provedor 1… Provedor 9. No gráfico, nota-se que o Provedor 1 e o Provedor 4 registaram maiores ocorrências com 18,069 que corresponde a 49,7% e 16071 que corresponde a 44,2%, respectivamente. A maior parte de ocorrências registadas nos provedores são de IPs relacionados a actividades na *Darknet*.

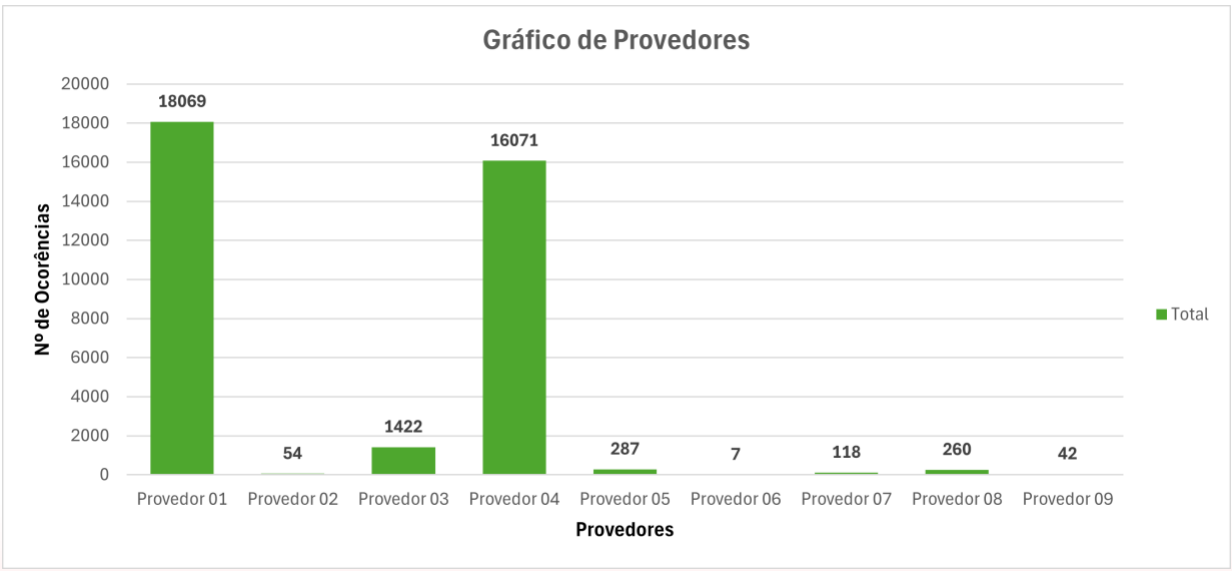

Figura 26: Número de ocorrências por provedores (2025).

O gráfico abaixo representa o período, em que foram registadas as ocorrências. Durante o período em análise, constatou-se que o pico de registo das ocorrências é no intervalo das 01:00H (01:00 AM) às 14:00H (02:00 PM).

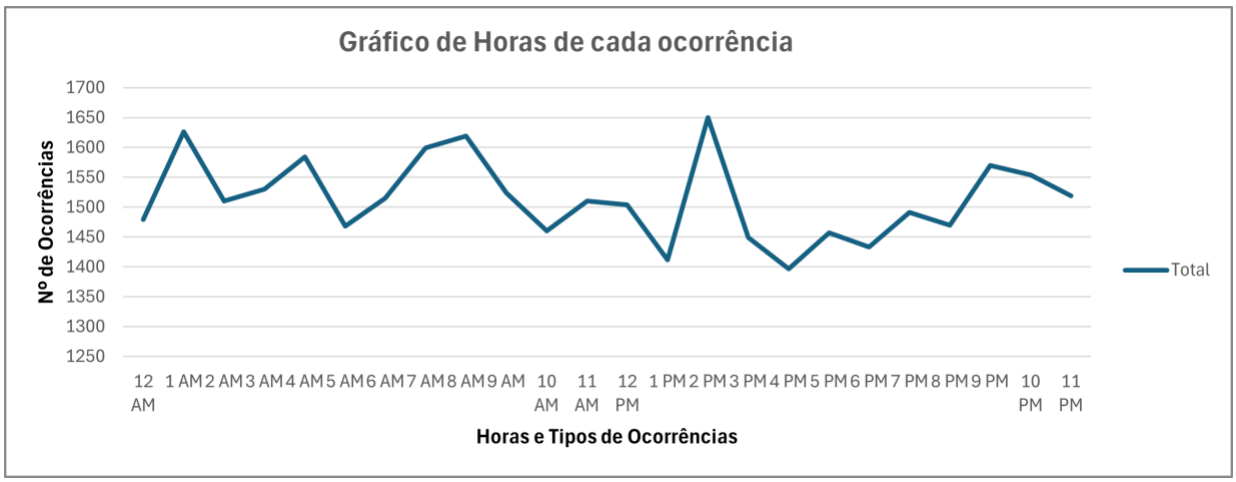

Figura 27: Tempo de registo das ocorrências (2025)

5 REDE NACIONAL DE CSIRTS

A PENSC orienta para que todos reguladores sectoriais estabeleçam os CSIRTs Sectoriais, as Províncias devem criar os respectivos CSIRTs Provinciais, os municípios são instados a estabelecer os CSIRTs Municipais e por sua vez todas instituições públicas e privadas devem criar os CSIRTs institucionais.

A Rede Nacional de CSIRTs é coordenada pelo CSIRT Nacional e se apresenta com o modelo hierárquico apresentado na figura 28.

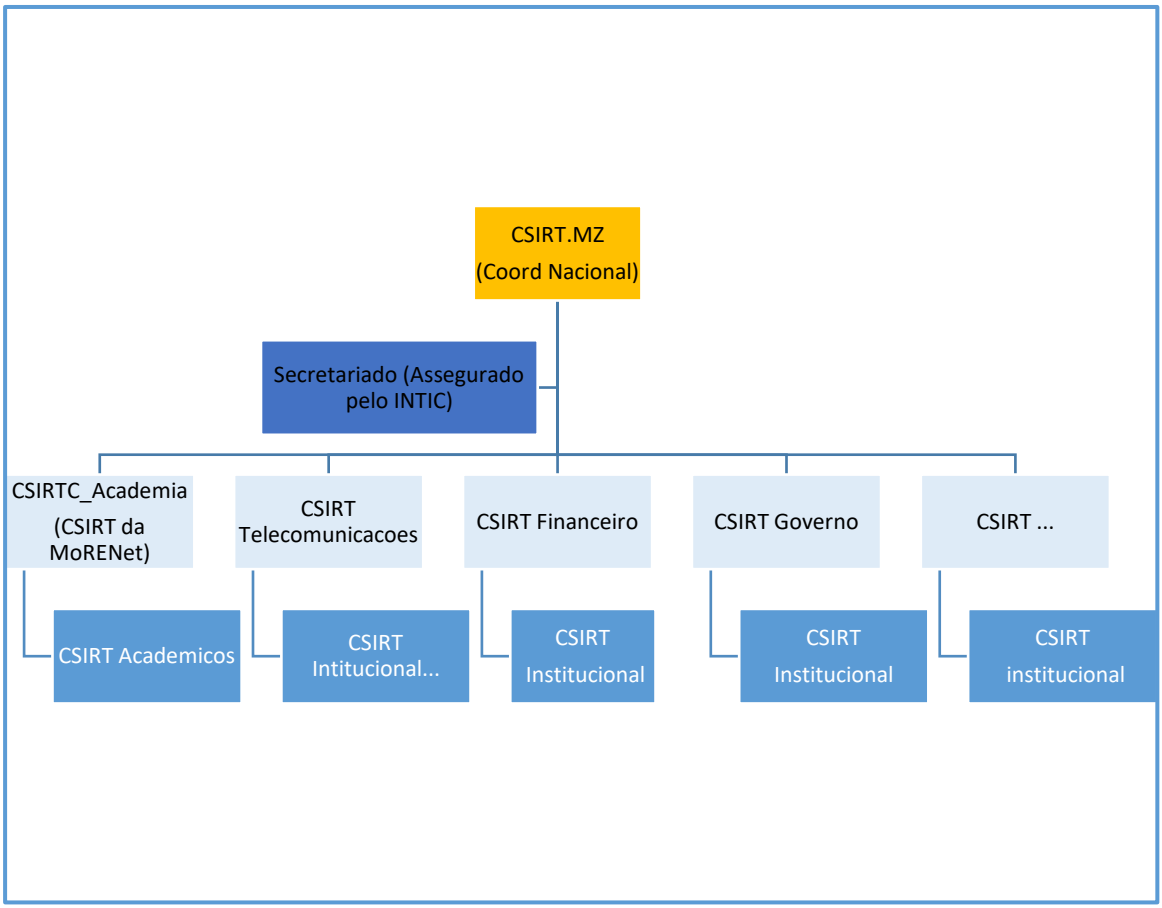

Figura 28: Modelo Hierárquico da Rede Nacional de CSIRT

A Rede Nacional de CSIRTs está em processo de consolidação neste momento, para além do CSIRT Nacional, conta com o CSIRT do Governo, o CSIRT da Rede de Instituições de Ensino Superior e de Investigação de Moçambique (MoRENet) geridos pelo INAGE, o CSIRT do Instituto Nacional das Comunicações de Moçambique (INCM), o CSIRT do Centro de Desenvolvimento de Sistemas de Informação de Finanças (CEDSIF), o CSIRT da Província de Inhambane, e o CSIRT da Província de Tete, estando ainda em curso o estabelecimento dos CSIRTs sectoriais das Finanças, das Telecomunicações e de Energia.

Encontram-se em processo de criação os CSIRT do Banco de Moçambique, Ministério da Defesa Nacional, Universidade Eduardo Mondlane Hidrelétrica de Cahora Bassa, Instituto Nacional de Segurança Social e os CSIRT dos sectores das Telecomunicações, Energia e Financeiro;

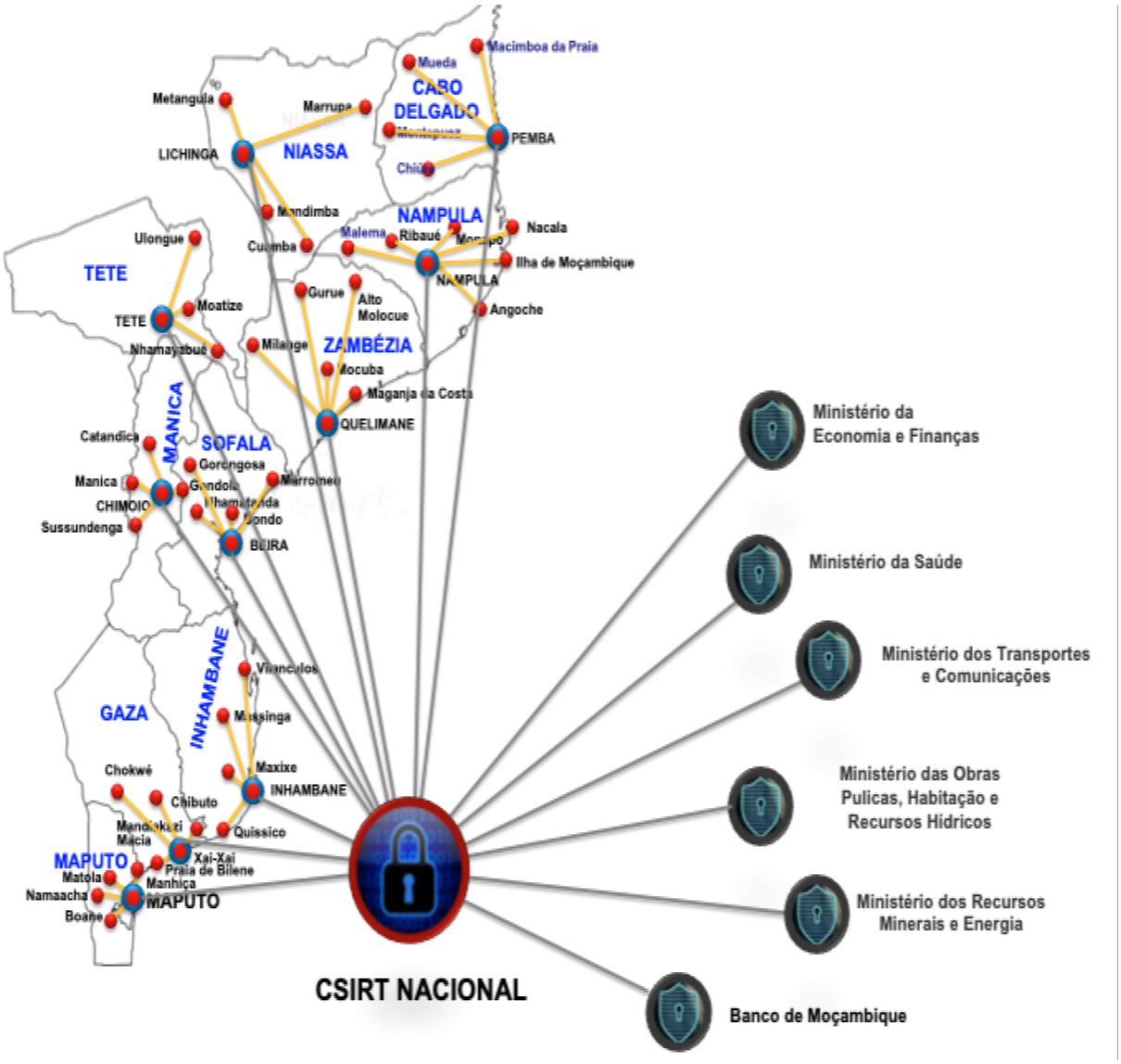

Figura 29: Rede Nacional de CSIRT

6 IMPACTO DO NCSIRT.MZ NA CLASSIFICAÇÃO DE MOÇAMBIQUE NO ÍNDICE GLOBAL DE SEGURANÇA CIBERNÉTICA (GCI) - 2024

O Índice Global de Segurança Cibernética, em inglês designado de "*Global Cybersecurity Index* (*GCI*)", é uma iniciativa da União Internacional de Telecomunicações (ITU), uma agência especializada das Nações Unidas, tendo como objectivo medir o compromisso dos países em relação a segurança cibernética, através da implementação de medidas relevantes.

O Índice Global de Segurança Cibernética (GCI) tonou-se uma referência credível que mede o compromisso dos países com a segurança cibernética a nível global, para aumentar a consciencialização sobre a importância e as diferentes dimensões da segurança cibernética. Como a segurança cibernética tem um amplo campo de aplicação, abrangendo muitas indústrias e vários sectores, a Organização Mundial de Telecomunicações (ITU) estabeleceu um critério para medir o nível de desenvolvimento ou envolvimento de cada país, sendo avaliado em cinco pilares nomeadamente: **(i) Medidas Legais**, **(ii) Medidas Técnicas**, **(iii) Medidas Organizacionais**, **(iv) Desenvolvimento de Capacidades** e **(v) Cooperação**. Este relatório é baseado em colecta de informações comprováveis, que culmina com a publicação de um relatório que atribui uma pontuação global.

O facto da Estratégia Nacional de Segurança Cibernética contemplar todos pilares definidos no GCI e definir de forma clara, o que o pais pretende seguir na melhoria do ecossistema de segurança cibernética e outras medidas tais como: Estabelecimento do CSIRT Nacional, adopção do modelo de maturidade em segurança cibernética (SIM3), realização da Reunião Anual de CSIRTs e a realização de campanhas de consciencialização a vários níveis, treinamentos, conferências e *workshops* sobre segurança cibernética, criação e gestão de CSIRTs que servem de mecanismos de colaboração regular entre os membros da Rede Nacional de CSIRTs e especialistas de segurança cibernética, para além do estabelecimento de mecanismos de cooperação internacional e ajuda mútua foi um dos factores preponderantes para que na 5ª edição do GCI[1], publicado em 2024, Moçambique obtivesse 66.05 pontos, encontrando-se posicionada no 3º nível que é dos países em estabelecimento, que representa os países que obtiveram uma pontuação global de pelo menos 55/100 pontos.

A assinatura de acordos e memorandos de entendimento bilaterais com países como Gana, Ruanda, Africa do Sul, Eswatini, Portugal, Brasil entre outros, assim como a participação do nCSIRT.mz em fóruns multilaterais a nível regional e global, como o caso do GFCE, FIRST, AfricaCERT, SmartAfrica, designação de Moçambique como Ponto Focal Técnico das Nações Unidas no âmbito do *Open-Ended Working Group on ICTs* das Nações Unidas entre outros, que garantem uma capacitação contínua dos quadros do nCSIRT.mz, troca de informação e experiencias em matérias de segurança cibernética, são outros factores que contribuíram para que Moçambique registasse uma subida de 41.86 pontos na 5ª edição do GCI, publicada em

[1] International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th edition). Geneva: ITU. Acessado em 12 de Outubro de 2024: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

2024, em comparação a 4ª edição do GCI, publicada em 2020, conforme se pode notar na tabela a seguir. A tabela 9 apresenta a pontuação de Moçambique em 2020 e 2024 no GCI.

***Tabela 9**: Pontuação de Moçambique em 2020 e 2024*

#	Ano	Legais	Técnicas	Organizacionais	Desenvolvimento de capacidade	Cooperação	Total
1	2020	7.46	8.19	4.62	3.92	0.0	24.19
2	2024	13.92	11.83	15.79	7.93	16.58	66.05
3	Variação						
4		6.46	3.64	11.17	4.01	16.58	41.86

Fonte: Relatório de Avaliação do Desempenho de Moçambique no Índice Global de Segurança Cibernética 2020.2024, INTIC, 2024.

No pilar sobre as Medidas do Quadro Legal, o nCSIRT.Mz participou na elaboração do Regulamento de Registo e Licenciamento de Provedores Intermediários de Serviços Electrónicos e de Operadores de Plataformas Digitais, aprovado em Outubro de 2023, elaboração da Convenção das Nações Unidas Contra Crimes Cibernéticos, adoptada em 9 de Agosto de 2024 e participa nos seguintes instrumentos em elaboração: Lei de Segurança Cibernética, Lei sobre Crimes Cibernéticos, Lei de Protecção de Dados, Regulamento de Desenvolvimento, Contratação e Operação de Plataformas de Computação em Nuvem, Regulamento de Construção e Operação de Centros de Dados, Revisão do Regulamento do Quadro de Interoperabilidade de Governo Electrónico, criação de um *framework* de governação de dados e outros regulamentos atinentes a ratificação das convenções internacionais como o caso da Convenção de Budapest em Moçambique foi convidado a participou no Comité da Convenção de Budapeste desde Junho de 2024 juntando-se ao concerto de Nações que cooperam na prevenção e no combate a crimes cibernéticos. O Gráfico Comparativo da Evolução de Moçambique no Índice Global de Cibersegurança que traduz a tabela 9 é apresentado a seguir.

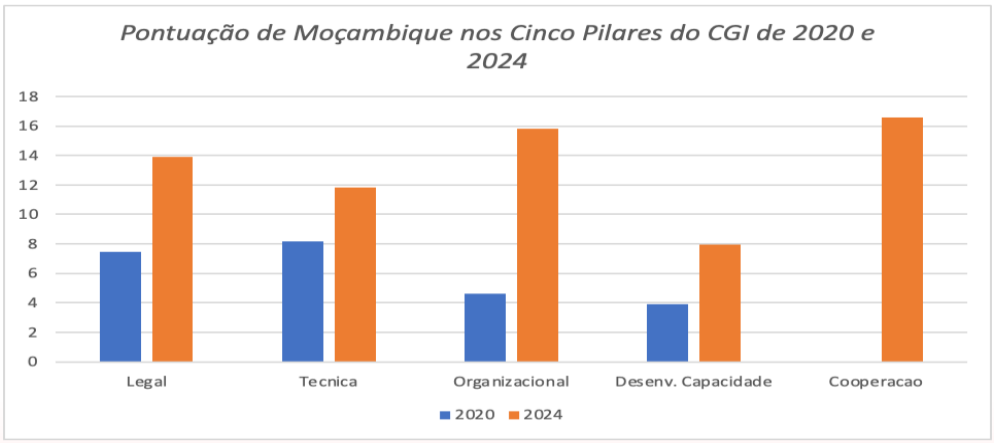

Figura 30: Gráfico Comparativo da Evolução de Moçambique no Índice Global de Cibersegurança

Fonte: Relatório de Avaliação do Desempenho de Moçambique no Índice Global de Segurança Cibernética 2020-2024, INTIC, 2024

7 PREVENÇÃO E COMBATE OS CRIMES CIBERNÉTICOS

A consciencialização é o primeiro passo para a mudança com vista a criação de uma cultura individual e colectiva para adopção de um comportamento seguro e responsável no uso das plataformas digitais.

7.1 Consciencialização Pública em Segurança Cibernética

Torna-se imperioso, para o efeito, implementar campanhas de consciencialização pública sobre a segurança no ambiente digital e incluir a literacia digital nos currículos escolares, desde os níveis mais básicos. As campanhas de consciencialização pública em Moçambique são projetadas para o sector público a vários níveis, sector privado, academia, as crianças e sobre tudo para atender às necessidades específicas da população, considerando o contexto socioeconômico, os níveis de alfabetização digital e as desigualdades de acesso à tecnologia.

Neste âmbito o CSIRT Nacional realizou em 2023 campanhas de consciencialização pública com foco para crianças e jovens em Fevereiro, Abril, Junho e Outubro abrangendo de 4.500 pessoas.

A figura 30 mostra da palestra estava inserida nas comemorações do Mês da Internet Mais Segura em Fevereiro de 2024 e tinha como objectivo consciencializar a comunidade académica da Escola Génios, em particular aos alunos, pais e encarregados de educação, professores e aos funcionários administrativos sobre as boas práticas para a utilização segura e responsável da Internet. Participaram na palestra cerca de 450 pessoas, de entra elas, pais e encarregados de educação, alunos da 1ª à 10ª Classes, professores e funcionários administrativos da Escola.

Figura 31: Momento de consciencialização a comunidade académica da Escola Primária e Secundária Génios, localizada no Município da Cidade da Matola, Província de Maputo.

A figura abaixo ilustra o momento do Webinar sobre a Consciencialização a Crianças e Jovens Sobre o Comportamento Seguro e Responsável no Ambiente Digital, realizado no dia 17 de Outubro de 2024.

Figura 32: Webinar sobre a Consciencialização a Crianças e Jovens Sobre o Comportamento Seguro e Responsável.

Neste ano foi realizada no Mês de Fevereiro – considerado o Mês da Internet Mais Segura uma campanha de consciencialização pública que abrangeu mais de 1.500 pessoas dos sectores público e privado, academia. Sociedade Civil e em particular a crianças e jovens.

A campanha iniciou com a publicação da Exortação de S.Excia. Ministro das Comunicações e Transformação Digital por Ocasião da Celebração do Mês da Internet Mais Segura, com vista a exortar as entidades públicas e privadas, assim como a sociedade em geral para adoptarem as diretrizes imanadas pelos instrumentos orientadores sobre segurança cibernética e práticas seguras com vista ao fortalecimento do ecossistema de segurança cibernética em Moçambique.

Figura 33: Exortação de S.Excia. o Ministro das Comunicações e Transformação Digital

No dia 21 de Fevereiro de 2025, foi realizado o Webinar para a **Divulgação dos Cursos Online Sobre Comportamento Seguro no Espaço Cibernético.** em colaboração com CNSC de Portugal, com vista a promoveu a aderência dos quatro cursos online em Português nomeadamente: (i) Cidadão Ciberseguro; (ii) Cidadão ciberinformado; (iii) Consumidor ciberseguro e (iv) cidadão cibersocial, lançados em 2022 em que já participaram cerca de 1.500 cidadãos moçambicanos.

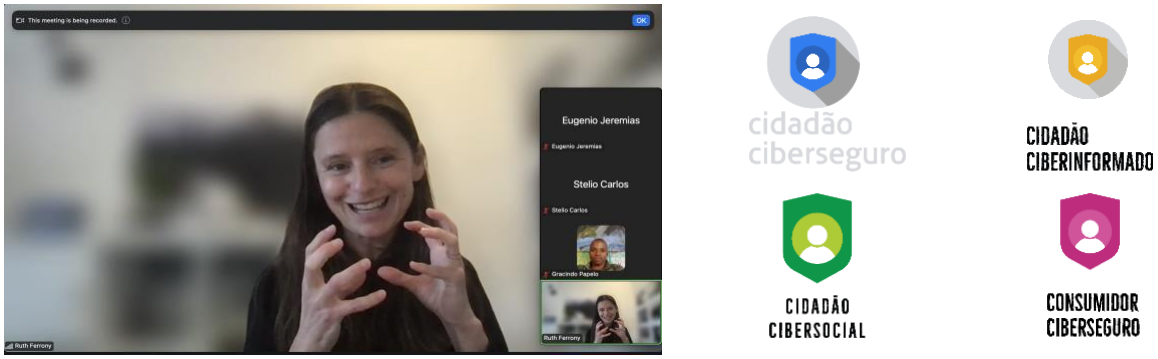

Figura 34: Momentos da apresentação feita pela Oradora Dra. Rhut Ferrony da CNCS de Portugal

No dia 24 de Fevereiro de 2025, realizou-se a palestra sobre a Rede Nacional de CSIRTs (webinar CSIRTs em Acção) que tinha como objectivo dinamizar e incentivar a criação de Equipas de Resposta a Incidentes de Segurança Cibernética (CSIRTs) sectoriais, províncias, municipais e institucionais e o estabelecimento da Rede Nacional de CSIRTs enquadrada na iniciativa número 3 da PENSC. Esta palestra sobre a Rede Nacional de CSIRTs tinha como objectivo dinamizar e incentivar a criação de Equipas de Resposta a Incidentes de Segurança Cibernética (CSIRTs) sectoriais, províncias, municipais e institucionais e o estabelecimento da Rede Nacional de CSIRTs enquadrada na iniciativa número 3 da PENSC.

As Palestras de consciencialização sobre uso mais seguro da Internet foram realizadas na Escola Secundária Josina Machel e na Escola Secundária Francisco Manyanga na Cidade de Maputo e na Escola Secundária Maria Ana Mogas, localizada na Cidade da Matola com participação de 1.477 jovens e adolescentes.

Figura 35: Momentos da Palestra na Escola Secundária Maria Ana Mogas – Cidade da Matola

Realizou-se no dia 27 de Fevereiro de 2025 o Webinar sobre a Convenção de Budapest e Convenção das Nações Unidas contra o uso de Tecnologias de Informação e Comunicação para propósitos criminais que teve como objectivo partilhar e trocar experiências sobre a Convenção de Budapest e Convecção das Nações Unidas contra o uso de Tecnologias de Informação e Comunicação para propósitos criminais e sensibilizar os participantes sobre a relevância das convenções internacionais no combate aos crimes cibernéticos e seu impacto na legislação e estratégias de segurança cibernética e contou com a participação de um universo de 161 pessoas, com destaque o sector público e privado, academia, sociedade civil e cidadão no geral.

Figura 36: Momentos da Realização do Webinar sobre a Convenção de Budapest e Convenção das Nações Unidas contra o uso de Tecnologias de Informação e Comunicação para propósitos criminal

No âmbito das celebrações do Mês da Mulher, realizou-se no dia 14 de Março de 2025, na sala de reuniões do INTIC, IP, o webinar "Mulheres na Transformação Digital – Desafios e Oportunidades", om participação de 82 pessoas.

Figura 37: Oradoras no Webinar

No âmbito das celebrações do Mês da Mulher, realizou-se no dia 14 de Março de 2025, **Webinar sobre Desenvolvimentos da Inteligência Artificial no Mundo:** Desafios e Oportunidades para Moçambique, alusivo ao Dia da Mulher Moçambicana, com participação de 67 partipantes.

No âmbito das celebrações do Mês da Mulher, realizou-se no dia 27 de Março de 2025, na sala de reuniões do INTIC, IP, o webinar " **Proposta de Lei de Protecção de Dados Pessoais** ". com a participação de um universo de 50 pessoas.

Figura 38: Webinar Sobre Proposta de Lei de Protecção de Dados

No âmbito da celebração do 2º Aniversário do nCSIRT, no dia 15 de Abril de 2025 foi realizado o **Webinar Sobre Como Construir Resiliência Cibernética** que abordou sobre soberania de dados de construção de CSIRTs/SOCs e das principais ferramentas para a sua operação com participação de 30 pessoas. Enfatizou-se que as organizações muitas vezes, adiantam com a automação, sem processos maduros e integração entre ferramentas, correndo o risco de criar um CSIRT ou SOC que responde rápido, mas responde mal. No processo de estabelecimento de CSIRTs ou SOCs o ponto central é o equilíbrio entre tecnologia, processos e pessoas. Muitas vezes, o foco inicial está excessivamente voltado para ferramentas, enquanto a maturidade dos CSIRTs ou SOCs depende fortemente de uma estrutura de governança bem definida e equipes capacitadas.

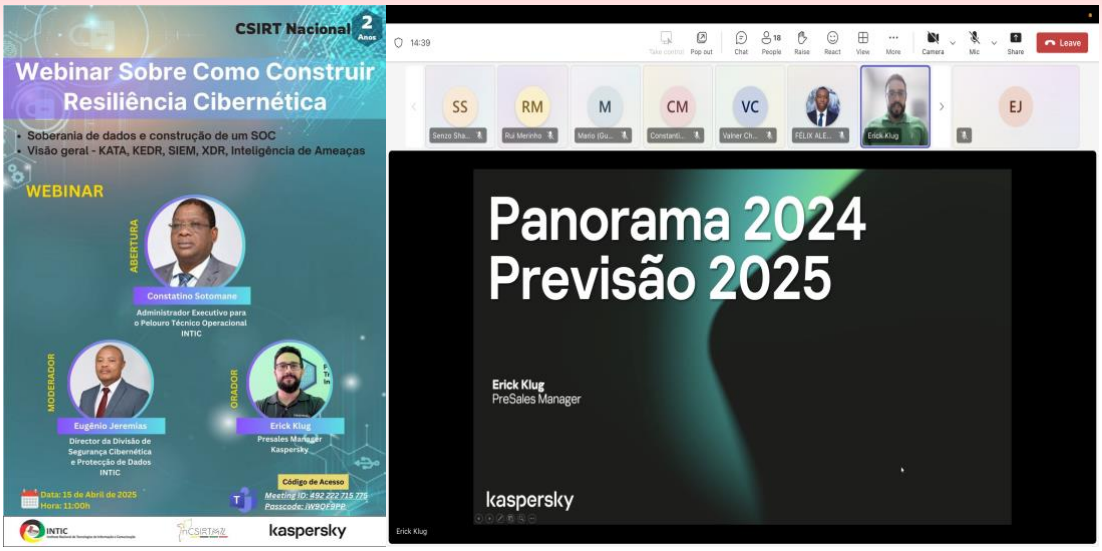

Figura 39: Webinar Sobre Como Construir Resiliência Cibernética

7.2 Combate aos Crimes Cibernéticos

No âmbito da Prevenção e Combate os Crimes Cibernéticos foram levados a cabo várias iniciativas a destacar as seguintes:

- Realização do Levantamento de Necessidades no Âmbito do Combate a Crimes Cibernéticos, apoiado pelo Escritório das Nações Unidas sobre Drogas e Crimes (UNODC), que produziu recomendações com base nas quais esta a ser elaborado um plano de acção de 3 anos;
- Participação nas iniciativas para o combate de Crimes Cibernéticos promovidos pela INTERPOL e pelo Projecto GLACY+ do Conselho da Europa que esta apoiou na avaliação da legislação existente em matéria de crimes cibernéticos no processo de elaboração da Lei de Crimes Cibernéticos, assegurando o alinhamento com a Convenção de Budapeste;
- Submissão da manifestação de interesse para adesão a Iniciativa Internacional para o Combate do *Ransomware* iniciativa que visa erradicar esta ameaça a nível global;
- Participação no Comité Técnico da Convenção de Budapeste em Junho de 2024 como país observador;
- Participação na Comissão Ad Hoc das NU de elaboração da Convenção das Nações Unidas Contra o Uso de TIC para Propósitos Criminais e nos trabalhos do *Open-Ended Working Group on ICT* das Nações Unidas;
- Adopção do Framework das Nações Unidas de Comportamento Responsável dos Estados no Espaço Cibernético.

Estas ações reflectem um compromisso significativo que o país tem com a cooperação internacional, o fortalecimento legal e a implementação de políticas eficazes para combater crimes cibernéticos, alinhando-se às melhores práticas globais e assegurando o comportamento responsável dos Estados no ambiente digital.

8 PUBLICAÇÕES DO NCSIRT.MZ

No âmbito da divulgação de informações sobre boas prática de segurança cibernética e procedimentos para o ecossistema de segurança cibernética em Moçambique, o nCSIRT.mz publicou este ano vários panfletos com diversas informações para técnicos e cidadão no geral, com destaque: Relatório de Avaliação do Desempenho de Moçambique no Índice Global de Segurança Cibernética 2020-2024 e Taxonomia da Rede Nacional de CSIRT: Classificação de Incidentes, ilustrados na figura 40; Perfil e Responsabilidades dos Técnicos a Nível Central, Sectorial, Provincial e Institucional no Âmbito do Cumprimento da Política e Estratégia Nacional de Segurança Cibernética, ilustrados na figura 41 e Relatório Nacional de Avaliação de Riscos Cibernéticos, ilustrados na figura 42 e 43.

Figura 40: Documento da Taxonomia da Rede Nacional de CSIRT.

Figura 41: Publicação sobre o Perfil e Responsabilidades dos Técnicos a Nível Central, Sectorial, Provincial e Institucional

Figura 42: Relatório de Avaliação de Moçambique no Índice Global de Segurança Cibernética 2020-2024

Figura 43: Ilustração do Relatório Nacional de Avaliação de Riscos Cibernéticos.

9 Acções em Curso e Perspectivas para 2025

Com vista a consolidar o nCSIRT.mz, estão em curso as seguintes acções:

- Realizar campanhas públicas de consciencialização sobre segurança cibernética maior dinamismo com a realização de acções em larga escala, incluindo a utilização de meios radiofónicos, televisivos e redes sociais (médias digitais), com conteúdo informativo e educacional, incluindo a utilização de algumas línguas locais;
- Estão previstas para 2025 acções de capacitação de 200 quadros em matérias especificas de segurança cibernética, este número será aumentado com a formação a ser realizada com o apoio de parceiros nacionais e internacionais;
- Participar junto as instituições de ensino na revisão de currículos académicos para introdução de cursos de graduação e pós-graduação, assim como o desenvolvimento de capacidade técnico-operacional, pesquisa e inovação em matérias de segurança cibernética que são parte da Estratégia Nacional de Ciência, Tecnologia e Inovação, aprovada este ano pelo Governo, com vista a introdução de cursos específicos de segurança cibernética nas Instituições de Ensino Superior e nas Instituições de Ensino Técnico Profissional e de acções de desenvolvimento de produtos e serviços de segurança cibernética nas instituições de investigação científica, pesquisa e desenvolvimento que, se concluídas com sucesso entre este e o próximo ano, poderão levar Moçambique aos níveis acima;
- Definição da arquitectura do ecossistema da Rede Nacional de CSIRT;
- Alocação e adequação do espaço para operação do nCSIRT.mz;
- Melhorar a capacidade e qualidade de produção de relatórios sobre segurança cibernética no país;
- Elaborar um *framework* de segurança cibernética para Moçambique;
- Estabelecer pelo menos 2 centros de partilha de informação (*Information Sharing and Analysis Centers-ISACs*);
- Reforçar a equipa do nCSIRT.mz com a integração de 6 (seis) especialistas;
- Aquisição do equipamento e ferramentas para melhorar a operação do nCSIRT.mz;
- Participar em eventos para troca de experiências e participação em fóruns de segurança cibernética a nível Nacional, Regional e Internacional.

As ações para consolidar o nCSIRT.mz incluem campanhas de consciencialização, capacitação de quadros especializados, integração da segurança cibernética nos currículos académicos, criação de centros de partilha de informação (ISACs) e reforço da infraestrutura e equipa técnica. Além disso, destaca-se a elaboração de um *framework* nacional e a participação em fóruns internacionais, fortalecendo a capacidade operacional e posicionando Moçambique no combate às ameaças cibernéticas.

10 CONSTRANGIMENTOS E DESAFIOS DO NCSIRT.MZ

O nCSIRT.mz enfrenta diversos constrangimentos e desafios incluindo:

- Falta de coordenação adequada entre o nCSIRT.mz e outras entidades públicas e privadas devido a interesses e prioridades diferentes;
- Limitação de profissionais qualificados, ferramentas de monitoramento, infra-estrutura e recursos adequados para o funcionamento do nCSIRT.mz;
- Falta de um quadro regulatório para definir responsabilidades e direitos em incidentes de segurança;
- Falta de recursos financeiros para realização de actividades de sensibilização para cibersegurança e a consciencialização de sua importância.

Os desafios enfrentados pelo nCSIRT.mz refletem obstáculos significativos que comprometem sua eficácia no fortalecimento da segurança cibernética no país. A falta de coordenação entre entidades públicas e privadas, devido a prioridades divergentes, impede uma resposta integrada e eficiente a incidentes de segurança. A escassez de profissionais qualificados, infraestrutura adequada e ferramentas de monitoramento limita a capacidade operacional do centro. Além disso, a ausência de um quadro regulatório dificulta a definição clara de responsabilidades, enquanto a restrição de recursos financeiros compromete ações essenciais de sensibilização e consciencialização sobre cibersegurança. Superar esses desafios exigirá investimentos coordenados, parcerias estratégicas e um compromisso contínuo com a capacitação e o desenvolvimento de políticas estruturadas.

11 CONCLUSÃO

A criação e operacionalização do nCSIRT.mz, em Moçambique, representa um marco significativo na promoção da segurança cibernética no país, alinhando-se com a Política Nacional e Estratégia de Segurança Cibernética. Ao longo do período de Abril de 2023 a Abril de 2025, diversas acções foram implementadas, como a formação de técnicos, o estabelecimento de parcerias internacionais e a introdução de ferramentas para a gestão de incidentes.

Apesar dos desafios, como a limitação de recursos e a necessidade de coordenação com outras entidades, os resultados positivos evidenciados pelo aumento na pontuação do Índice Global de Segurança Cibernética, demonstram o potencial do nCSIRT.mz para fortalecer a resiliência do país frente às ameaças cibernéticas. Assim, é imperativo que todos os *stakeholders* continuem a colaborar, investindo em capacitação e infraestrutura, para consolidar um ecossistema cibernético mais seguro e eficaz. A segurança cibernética não é apenas uma responsabilidade do nCSIRT.mz, mas de toda a sociedade Moçambicana.

É importante referir que o cenário das ameaças cibernéticas está em constante evolução, e novas tendências surgem constantemente. As táticas clássicas, como o *phishing* ou *ransomware*, estão a evoluir e a avançar à medida que os agentes de ameaças têm acesso a novos recursos.