UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE LETRAS E CIÊNCIAS SOCIAIS

DEPARTAMENTO DE CIÊNCIA POLÍTICA E ADMINISTRAÇÃO PÚBLICA

CURSO DE LICENCIATURA EM ADMINISTRAÇÃO PÚBLICA

Análise dos ataques cibernéticos ao governo electrónico (2020-2023): o papel do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC)

Licenciando: Alberto António Matsimbe

Supervisor: Doutor Renato Augusto Pereira

Maputo, Outubro de 2025

Alberto António Matsimbe

Análise dos ataques cibernéticos ao governo electrónico (2020-2023): o papel do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC)

Monografia apresentada à Faculdade de Letras e Ciências Sociais da Universidade Eduardo Mondlane como requisito parcial para obtenção do grau de Licenciatura em Administração Pública

Supervisor: Doutor Renato Augusto Pereira

Maputo, Outubro de 2025

Alberto António Matsimbe

Análise dos ataques cibernéticos ao governo electrónico (2020-2023): o papel do Instituto Nacional da Tecnologia de Informação e Comunicação (INTIC)

Trabalho de Fim de Curso apresentado em cumprimento dos requisitos exigidos para obtenção do grau de Licenciatura em Administração Pública, na Faculdade de Letras e Ciências Sociais da Universidade Eduardo Mondlane.

Data de Aprovação: _____/_____/2025

Mesa de Júri:

_____

O Presidente

_____

O Supervisor

_____

O Oponente

Maputo, Outubro de 2025

DECLARAÇÃO DE HONRA

Declaro por minha honra, que este trabalho de fim de curso nunca foi apresentado, na sua essência, para a obtenção de qualquer grau académico, e que constitui o resultado da minha investigação, estando indicadas no texto e nas referências bibliográficas as fontes que utilizei para a sua elaboração.

O Licenciando

_____

(Alberto António Matsimbe)

Maputo, Outubro de 2025

EPÍGRAFE

"Os ataques cibernéticos contra os sistemas de uma nação podem fazer mais do que desactivar serviços ou roubar dados, eles podem abalar a fé dos cidadãos no próprio governo."

Richard A. Clarke (2010)

DEDICATÓRIA

Aos meus pais, Zefanias Alberto Matsimbe e Odete António Porteiro, pois é graças ao vosso esforço que hoje posso concluir esta etapa da minha formação.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão ao meu supervisor, Renato Augusto Pereira (PhD), pela sua inestimável orientação, apoio e incentivo durante todo o processo de elaboração desta monografia. Agradeço a paciência, as valiosas sugestões e a constante disponibilidade para me auxiliar na superação dos desafios encontrados. Sem a sua expertise e dedicação, este trabalho não seria possível.

Sou grato à minha família e amigos pelo apoio incondicional durante toda a minha trajectória académica. Agradeço em especial aos meus pais, Zefanias Alberto Matsimbe e Odete António Porteiro, por acreditarem em mim e me incentivarem a sempre buscar meus sonhos. Aos meus irmãos, Ayanda, Kelvin e Luena, mano vos ama! Agradeço também aos meus tios Pedro Matsimbe e Lourino Matsimbe, Nito e Zelito Porteiro e finalmente a minha tia Fátima Porteiro, pelo suporte. Ao meu primo que carinhosamente trato por irmão, Fernando Benedito Porteiro, por sempre estar do meu lado.

Agradeço igualmente aos meus amigos, Abílio Muthemba, António Felisberto Criva, Aristides Guirringane, Gesso Matsinhe, Edmilson Ngoca e Jaime Ngoca, pelo companheirismo e por me proporcionarem momentos de descontracção e alegria, em especial à minha amiga Vinódia Arlindo Maxlhope, pelo auxílio em disponibilizar o seu laptop sempre que necessário. Agradeço também aos meus colegas de curso, Angelina António, Cátia Rangel, Hulda Latifo, Muniz Chiparanga e Nidiloide da Costa, pelas valiosas discussões e colaboração durante a pesquisa. Agradeço especialmente ao Pedro Banze, pela ajuda na colecta de dados e análise dos resultados.

Finalmente, agradeço à Universidade Eduardo Mondlane por me proporcionar a oportunidade de realizar esta monografia. Agradeço especialmente ao departamento de Ciência Política e Administração Pública pela aprendizagem que tive ao longo destes 4 anos e pela minha formação como homem e profissional.

RESUMO

O presente trabalho de pesquisa é intitulado “Análise dos ataques cibernéticos ao governo electrónico (2020-2023): o papel do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC)”. Esta pesquisa analisa as ameaças digitais enfrentadas pelo governo electrónico em Moçambique, identificando os principais ataques cibernéticos, os factores que tornam o e-GOV vulnerável, as suas consequências, bem como os desafios enfrentados pelo INTIC na prevenção e mitigação desses incidentes. A pesquisa insere-se no contexto da Administração Pública moçambicana, que tem adoptado o governo electrónico (e-GOV) como instrumento de modernização administrativa, visando a melhoria da eficiência, transparência e prestação de serviços públicos digitais. Contudo, a crescente digitalização da administração pública expõe o Estado a novas ameaças cibernéticas que podem comprometer a continuidade e a segurança dos serviços públicos. Nesse cenário, o INTIC assume um papel estratégico como órgão responsável pela implementação de políticas, normas e estratégias de segurança cibernética, sendo, portanto, fundamental para a consolidação e protecção da governação electrónica no país. A relevância do estudo reside na necessidade de fortalecer a segurança digital da Administração Pública, assegurando a integridade, confidencialidade e disponibilidade das informações governamentais. Do ponto de vista metodológico, trata-se de uma pesquisa básica, de abordagem qualitativa e natureza descritiva, utilizando o estudo de caso como procedimento técnico e, como técnicas de colecta de dados, a pesquisa bibliográfica, documental e a entrevista semiestruturada. Fundamenta-se na Teoria de Sistema, partindo do entendimento de que o e-GOV é um sistema aberto, que interage com diferentes sectores da sociedade e, por isso, pode tornar-se vulnerável a ataques que ameaçam os dados das instituições e dos cidadãos. Os resultados demonstram que os ataques cibernéticos representam um desafio crescente para a Administração Pública, exigindo acções coordenadas e políticas eficazes do INTIC e de outras entidades governamentais para garantir a segurança da informação e a confiança dos cidadãos na governação digital.

Palavras-Chave: Administração Pública, ataques cibernéticos, governo electrónico, INTIC

ABSTRACT

This research analyzes the digital threats faced by electronic government (e-GOV) in Mozambique, identifying the main types of cyberattacks, the factors that make e-GOV vulnerable, their consequences, as well as the challenges faced by INTIC in preventing and mitigating such incidents. The study is situated within the context of the Mozambican Public Administration, which has adopted electronic government as an instrument for administrative modernization aimed at improving efficiency, transparency, and the delivery of digital public services. However, the growing digitalization of public administration exposes the State to new cyber threats that may compromise the continuity and security of public services. In this context, INTIC plays a strategic role as the institution responsible for implementing cybersecurity policies, standards, and strategies, and is therefore essential for the consolidation and protection of electronic governance in the country. The relevance of this study lies in the need to strengthen the digital security of Public Administration by ensuring the integrity, confidentiality, and availability of governmental information. Methodologically, this is a basic research with a qualitative and descriptive approach, using the case study as a technical procedure and, as data collection techniques, bibliographic research, documentary analysis, and semi-structured interviews. The study is grounded in Systems Theory, based on the understanding that e-GOV is an open system that interacts with different sectors of society and, as such, may become vulnerable to attacks that threaten institutional and citizen data. The results show that cyberattacks represent a growing challenge for Public Administration, requiring coordinated actions and effective policies from INTIC and other governmental entities to ensure information security and maintain citizens' trust in digital governance.

Keywords: Public Administration, cyberattacks, electronic government , INTIC

SIGLAS E ABREVIATURAS

CFM – Caminhos de Ferro de Moçambique

CSIRC – Centros de Resposta a Incidentes de Segurança Computacional

DDoS – Distributed Denial of Service

DUAT – Direito de Uso e Aproveitamento da Terra

EGEM – Estratégia de Governo Electrónico de Moçambique

e-SISTAFE – Sistema Electrónico de Administração Financeira do Estado

GCI – Índice Global de Segurança Cibernética

GovNET – Rede Electrónica do Governo

INAGE – Instituto Nacional de Governo Electrónico

INCM – Instituto Nacional de Comunicações

INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação

MCTESTP – Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profissional

MTC – Ministério dos Transportes e Comunicações

NCRA – Avaliação Nacional de Risco Cibernético

NUIT – Número Único de Identificação Tributária

SADC – Comunidade de Desenvolvimento da África Austral

TGS – Teoria Geral dos Sistemas

TIC – Tecnologias de Informação e Comunicação

UA – União Africana

UE – União Europeia

UIT – União Internacional de Telecomunicações

SUMÁRIO

LISTA DE ILUSTRAÇÕES

Figuras

Quadro

Gráficos

CAPÍTULO I

1. Introdução

O presente trabalho de pesquisa tem como tema *análise dos ataques cibernéticos ao governo electrónico (2020 – 2023): O papel do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC).* O tema enquadra-se nos debates teóricos sobre a segurança do governo electrónico no Estado moçambicano.

O advento das Tecnologias de Informação e Comunicação (TIC) revolucionou todas as esferas da vida social dos cidadãos e o funcionamento das instituições que afectam directamente as suas vidas. Na esfera da gestão pública, as TICs desempenham um papel de suporte administrativo, bem como de ferramenta para uma participação do cidadão mais estratégica no processo de tomada de decisão, auxiliando na implementação e avaliação de políticas públicas e programas de governação (ROMÃO, 2023).

O uso das TICs serviu de intermediário por meio do qual os servidores ou gestores públicos disponibilizam seus serviços, organizam, armazenam e comunicam entre si, e com os cidadãos, com maior flexibilidade e transparência. Assim, com a popularização das TICs no mundo, tornou-se possível a rápida difusão e organização da informação, razão pela qual é actualmente um meio utilizado pela administração pública para prestação de serviços de modo flexível e qualitativo (JOÃO, 2023).

Em virtude do salto tecnológico, os órgãos da administração pública viram-se impelidos a passarem por transformações constantes, adequando suas gestões à modernização com o intuito de atender às necessidades da sociedade. Para isso, foi preciso que a administração pública investisse mais em equipamentos tecnológicos e na capacitação de seus gestores e colaboradores, de modo a melhorar a qualidade e eficiência de seus serviços, bem como possibilitar uma forma de comunicação mais directa com o cidadão (ROSANE et al., 2015).

Com as novas tecnologias, o espaço cibernético trouxe a conexão e a celeridade ao mundo moderno, mas também revelou as vulnerabilidades existentes nesse ambiente. Além do aumento de usuários, verificou-se um crescente número de ataques no ciberespaço, inclusive contra o

próprio Estado que podem afectar infra-estruturas críticas de um país, como telecomunicações, energia, finanças, água e transporte, trazendo grandes riscos, prejuízos e impactos na vida do cidadão (SEGUNDO, 2015).

Embora a revolução da informação tenha criado novas oportunidades, melhorado a eficiência organizacional e promovido uma conectividade global sem precedentes, ela também trouxe novas vulnerabilidades e ameaças não convencionais, com implicações sociais, económicas, políticas e de segurança. Por conseguinte, é importante estudar os ataques cibernéticos no governo electrónico (e-GOV), pois garantir a protecção de dados sensíveis dos cidadãos e do Estado assegura a continuidade de serviços públicos essenciais como emissão de documentos e atendimentos *online* e previne prejuízos financeiros causados por paralisações ou sequestro de sistemas. Além disso, permite que os órgãos públicos actuem em conformidade com a legislação e fortaleçam a capacidade do governo em desenvolver políticas de cibersegurança eficazes, compreender esses ataques também é essencial para proteger o país contra ameaças externas e manter a confiança da população nas instituições públicas (SANTOS, 2022).

No que concerne a organização, a pesquisa é constituída por V capítulos a saber:

- O primeiro capítulo, diz respeito a introdução, que apresenta a contextualização como forma de perceber em que contexto o estudo se insere, o problema da pesquisa, a pergunta de partida, o objectivo geral e específico, delimitação do tema pesquisado, a justificativa que mostra a relevância e a importância da realização da presente pesquisa; o quadro teórico e conceptual onde se faz a fundamentação teórica da pesquisa, apresenta-se os conceitos essenciais: ataques cibernéticos; ciberespaço; cibersegurança e governo electrónico;
- No segundo capítulo, faz-se a revisão da literatura, isto é, tipos de ataques cibernéticos que afectam o e-GOV, factores que tornam o e-GOV vulnerável aos ataques cibernéticos, consequências dos ataques cibernéticos no e-GOV, e os desafios no combate aos ataques cibernéticos.
- No terceiro capítulo apresenta-se a metodologia que foi usada para a realização desta pesquisa, onde se define o tipo e as técnicas de pesquisa;

- No quarto capítulo faz-se a discussão e análise de dados, essa fase será responsável por encabeçar todo debate sobre os ataques cibernéticos no e-GOV em Moçambique com a informação que se colheu na fase da recolha de dados;
- E no quinto e último capítulo é apresentado a conclusão, recomendações, referências bibliográficas incluindo apêndice e anexos.

1.1. Contextualização

A administração pública moçambicana passava por uma fase de reformas, entre 1990 e 2001, que tinham como foco as transformações do sector público, visando a melhoria da qualidade dos serviços disponibilizados pelo Estado à sociedade, bem como a facilitação da comunicação entre os cidadãos e o Estado. Com o objectivo de optimizar a prestação de serviços, tornando-os mais céleres e modernos, surgiu a necessidade de integrar as Tecnologias de Informação e Comunicação (TIC), as quais vêm se destacando, desde a década de 1990, como uma solução eficaz para os desafios da administração pública (ROMÃO, 2023).

Para este autor, as TICs permitem elevar a eficácia e eficiência da gestão pública, reduzir custos operacionais, diminuir a burocracia e combater a corrupção no aparelho do Estado. Esses factores levaram o governo moçambicano a incluir a criação do Governo Electrónico como uma das acções estratégicas da Componente dois (2) (Melhoria no Processo de Formulação e Monitoria de Políticas Públicas) da Reforma do Sector Público. Com efeito, o executivo moçambicano implementou a Estratégia de Governo Electrónico de Moçambique (EGEM), instrumento que estabelece as directrizes para o uso das TIC na administração pública. Ainda segundo o mesmo autor, a incorporação desses serviços tecnológicos revelou-se uma oportunidade para a transformação do aparelho do Estado, indo além da simples reorganização administrativa (ROMÃO, 2023).

Para João (2023), as TICs permitiriam conjugar a “reinvenção” da máquina administrativa do governo com a "desburocratização" da administração pública, o que resultaria na melhoria da vida do cidadão e das relações destes com as instituições governamentais. O autor citado refere que as primeiras acções desenvolvidas pela administração pública moçambicana, através do governo electrónico, estavam ligadas à prestação de serviços como: a emissão de Bilhete de Identidade, a Carta de Condução biométrica, Direito de Uso e Aproveitamento da Terra (DUAT),

Número Único de Identificação Tributaria (NUIT), Registo Criminal, criação de serviços como o Balcão de Atendimento Único (BAU)**,** o Sistema Electrónico de Administração Financeira do Estado (e-SISTAFE), assim como a disponibilização de informações dos principais órgãos do governo e o conjunto de legislação que regulam vários assuntos. Estas acções associaram-se à tendência para o desenvolvimento do governo electrónico na administração pública moçambicana.

Com o desenvolvimento das infra-estruturas de comunicação em Moçambique e o aumento exponencial dos usuários das TICs, a necessidade do uso da Internet não só facilitou o acesso a serviços públicos assim como tornou esta ferramenta útil para aproximação do Estado ao cidadão, contudo, os riscos decorrentes do uso da Internet existem, e estas estão directamente relacionadas à segurança dos dados electrónicos, os ataques cibernéticos constituem o principal perigo quando se trata de ameaças electrónicas (FERREIRA, 2021).

Os ataques cibernéticos ao e-GOV têm se tornado cada vez mais comuns, especialmente na África, onde muitos países estão digitalizando seus serviços públicos. Esses ataques acontecem quando criminosos tentam invadir sistemas do governo pela internet para roubar dados, travar serviços ou causar confusão. Muitas vezes, os alvos são sites e plataformas usadas para emitir documentos, pagar taxas, acessar serviços de saúde ou educação (FERREIRA, 2021).

O panorama dos ataques cibernéticos dirigidos ao e-GOV em Moçambique mostra um crescimento sustentado em volume e complexidade: os incidentes reportados pela Equipa Nacional de Resposta a Incidentes Cibernéticos (nCSIRT) do INTIC evidenciam centenas de milhares de ocorrências anuais, muitas das quais consistem em tentativas de *phishing, malware* (incluindo *ransomware),* ataques de negação de serviço (DDoS) e *defacement* de *sites* institucionais, que têm provocado desde paralisações temporárias de serviços até dificuldade de acesso a portais públicos críticos; o relatório operacional do nCSIRT detalha esses padrões e as zonas de maior incidência (INTIC, 2025).

A fonte citada acima avança que as causas subjacentes combinam factores técnicos e organizacionais: infra-estrutura ligada com falhas de actualização e correcção, configurações inseguras, ausência ou fraca implementação de políticas de segurança padrão, além de baixa literacia digital entre servidores e cidadãos que facilita engenharia social (*phishing)* elementos que a análise de diagnóstico de dados do governo e estudos académicos também destacam.

Os alvos mais frequentes no espaço do e-GOV incluem portais e serviços oferecidos por ministérios, instituições fiscais e financeiras, sistemas de autenticação e bases de dados públicas; ataques bem-sucedidos têm impacto directo na continuidade dos serviços, na confiança dos utilizadores e, em alguns casos, podem expor dados sensíveis ou obrigar desligamentos temporários para conter a ameaça (INTIC, 2023).

1.2. Problema de Pesquisa

O rápido crescimento e o acesso global às TICs, combinados com o avanço económico, resultaram em um expressivo aumento de usuários iniciantes, especialmente nos países em desenvolvimento. De fato, a maior taxa de crescimento de usuários da internet actualmente ocorre em regiões como Ásia e África (UIT, 2014). Esse fenómeno tem sido acompanhado por uma transformação digital nas esferas públicas e privadas, reflectindo-se directamente na adopção de soluções de e-GOV. No entanto, à medida que o ciberespaço se torna um componente essencial da estrutura social, política e económica desses países, ele também expõe vulnerabilidades críticas especialmente no que se refere à segurança cibernética.

O ciberespaço, por ser descentralizado e sem fronteiras físicas, conecta sistemas de todos os tipos e níveis. Com isso, os países em desenvolvimento passam a enfrentar ameaças cibernéticas similares às que desafiam nações mais tecnológicas, como *malwares, phishing*, ataques de negação de serviço (DDoS), *ransomware*, invasões a bancos de dados e ataques direccionados à infra-estrutura de e-GOV. Estes últimos têm sido particularmente preocupantes, já que os sistemas de governo electrónico envolvem dados sensíveis de cidadãos, informações fiscais, registos de saúde, sistemas de votação, serviços jurídicos e outras funções críticas do Estado (UNDOC, 2013, ITU, 2012).

A rápida digitalização dos serviços públicos, embora represente uma oportunidade única de democratização do acesso, redução da burocracia e fortalecimento institucional, também gera uma superfície de ataque cibernético mais ampla. Em muitos casos, essa transformação digital é implementada sem uma estratégia de cibersegurança robusta, deixando sistemas governamentais expostos a ataques que podem comprometer seriamente a confiança pública, a integridade institucional e até mesmo a soberania nacional. Países em desenvolvimento enfrentam uma

combinação de factores que agravam esse cenário: redes frágeis, infra-estruturas digitais mal projectadas, ausência de políticas de segurança da informação, legislação deficiente e escassez de profissionais qualificados na área de cibersegurança (IDG CONNECT, 2012).

Além disso, a capacidade institucional limitada e a falta de sensibilização, tanto entre os tomadores de decisão quanto entre os usuários finais, tornam esses Estados alvos mais fáceis para agentes maliciosos, incluindo grupos cibercriminosos, *hackers* activistas (*hacktivistas*) e até mesmo operações de espionagem cibernética patrocinadas por Estados estrangeiros (Idem, 2012). Ademais, muitos desses países enxergam a digitalização como uma solução imediata para diversos problemas socioeconómicos urgentes, e por isso priorizam a implementação técnica das soluções sem dar a devida atenção aos seus riscos de segurança (PAWLAK, 2014).

A pressa em aderir à "onda digital" muitas vezes impulsionada por pressões externas ou incentivos internacionais pode levar à adopção de plataformas e ferramentas sem avaliação crítica sobre sua segurança ou adequação ao contexto local. Em contrapartida, existe também uma resistência por parte de certos governos que vêem a regulação e a segurança cibernética como imposições de modelos ocidentais, dificultando a adopção de boas práticas internacionais (BURT et al., 2014).

A implementação progressiva do e-GOV em Moçambique, o Estado tem procurado modernizar a sua administração pública, tornar os serviços mais acessíveis e promover maior transparência. No entanto, essa digitalização também tem exposto o país a novos riscos, entre os quais se destacam os ataques cibernéticos (SANTOS, 2022).

Em 2022, Moçambique vivenciou um dos episódios mais marcantes de ataques cibernéticos da sua história recente, revelando fragilidades estruturais na segurança digital das instituições públicas. Entre os dias 21 e 22 de Fevereiro, diversos portais governamentais foram alvo de um ataque coordenado que provocou a interrupção parcial ou total de vários serviços públicos *online*. Entre as plataformas afectadas encontravam-se o Instituto Nacional de Gestão de Desastres (INGD), a Administração Nacional de Estradas (ANE), a Administração Regional de Águas do Sul, e o Instituto Nacional de Transportes Terrestres (INATTER), entre outras (Clube de Moçambique, 2022). Os invasores substituíram o conteúdo original desses portais por

mensagens de teor político e imagens intimidatórias, reivindicando a autoria sob o nome de "hackers do Iémen", o que sugere a ocorrência de um ataque de origem externa. Este incidente foi considerado sem precedentes em Moçambique, não apenas pela quantidade de instituições afectadas, mas também pelo impacto directo na continuidade e credibilidade dos serviços públicos digitais (Clube de Moçambique, 2022).

Esses acontecimentos expuseram a vulnerabilidade do e-GOV moçambicano e levantaram preocupações sobre a eficácia das medidas de segurança adoptadas pelo Estado e pelos órgãos responsáveis pela gestão das infra-estruturas digitais. Assim, emergiu a necessidade de compreender de que forma esses ataques afecta o funcionamento da administração pública digital e a confiança dos cidadãos nos serviços online.

Com base nesse contexto, formulou-se a seguinte questão de partida: como os ataques cibernéticos ao e-GOV em Moçambique afectam a continuidade dos serviços públicos digitais?

Objectivos

1.2.1. Geral

- Analisar os ataques cibernéticos ao governo electrónico (2020-2023);

1.2.2. Específico

- Indicar os tipos de ataques cibernéticos ao governo electrónico;
- Identificar os factores que tornam o governo electrónico vulnerável aos ataques cibernéticos;
- Apontar as consequências dos ataques cibernéticos ao governo electrónico;
- Descrever os desafios do INTIC no combate aos ataques cibernéticos.

1.3. Delimitação da pesquisa

A Pesquisa teve Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) como enfoque espacial, e como delimitação temporal os anos de 2020-2023. Entre 2020 e 2023, Moçambique enfrentou um aumento significativo nos ataques cibernéticos direccionados à administração pública, afectando directamente na confiança dos cidadãos aos serviços digitais e na segurança das informações existentes nesse sistema. O Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) desempenhou um papel central na resposta a esses desafios, liderando iniciativas para fortalecer a cibersegurança no país.

1.4. Justificativa

O avanço acelerado da transformação digital e a crescente adopção de plataformas electrónicas para a prestação de serviços públicos têm levado governos em todo o mundo a investir no desenvolvimento de sistemas de e-GOV. Em Moçambique, esse processo tem se intensificado nos últimos anos como parte de uma estratégia nacional voltada à modernização da administração pública, ao aumento da eficiência institucional e à ampliação do acesso da população aos serviços estatais (UIT, 2014).

A digitalização, nesse sentido, tem promovido uma aproximação significativa entre o Estado e os cidadãos, ao viabilizar o acesso a serviços como emissão de documentos, pagamentos de taxas, consultas públicas e outros mecanismos essenciais à vida civil (PAWLAK, 2014).

A crescente dependência de plataformas digitais torna as estruturas governamentais mais expostas a ameaças cibernéticas, como ataques de negação de serviço (*DDoS),* invasões a bases de dados, sequestro de sistemas (*ransomware*) e outras formas de comprometimento da infra-estrutura digital do Estado (ASLLANI, 2022).

Burt et al. (2014) acrescentam que essas ameaças colocam em risco a integridade, a confidencialidade e a disponibilidade das informações públicas e dos dados pessoais dos cidadãos, afectando directamente a confiança social nas iniciativas de governo digital.

Moçambique, assim como muitos países em desenvolvimento, enfrenta limitações significativas no campo da cibersegurança, incluindo infra-estrutura tecnológica deficiente, ausência de políticas públicas específicas e integradas, escassez de recursos humanos qualificados e baixos

níveis de sensibilização institucional sobre os riscos inerentes ao ciberespaço (IDG CONNECT, 2022).

Esse cenário de vulnerabilidade compromete a resiliência dos sistemas de e-GOV e limita o potencial transformador das tecnologias digitais no sector público. Neste contexto, a presente pesquisa se justifica pela necessidade de compreender o panorama actual da segurança cibernética em Moçambique, no período de 2020 à 2023, com foco específico nos ataques cibernéticos direccionados às plataformas de governo electrónico. A análise proposta visa identificar os principais tipos de incidentes cibernéticos no e-GOV, suas causas, impactos e as fragilidades estruturais que os possibilitaram, além de propor estratégias e recomendações para fortalecer a protecção dos sistemas públicos digitais

1.5. Enquadramento Teórico e Conceitual

1.5.1. Quadro teórico

Esta pesquisa enquadra-se na teoria de sistema. Ao considerar o governo electrónico como um sistema aberto que interage com diferentes atores (cidadãos, instituições e tecnologia), essa abordagem ajuda a compreender as diferentes relações que podem influenciar a ocorrência de ataques cibernéticos e a eficácia das respostas governamentais.

1.5.2. Teoria de Sistemas

A Teoria de Sistemas, desenvolvida a partir da biologia de Ludwig Von Bertalanffy e incorporada à Administração na década de 1950, introduziu uma visão holística e integrada das organizações. Ela entende a organização como um sistema aberto, formado por subsistemas interdependentes (tecnológico, humano, administrativo, legal etc.), que interagem entre si e com o ambiente externo. A eficiência e a eficácia organizacional dependem da harmonia dessas interacções, bem como da capacidade de adaptação diante de influências externas. Assim, ao contrário das teorias administrativas anteriores, de carácter mais mecanicista e fechado, a Teoria de Sistemas valoriza a interdependência, a retroalimentação (*feedback*) e a adaptação dinâmica como elementos centrais para a sustentabilidade organizacional (CHIAVENATO, 2009).

A Escola Sistémica é definitivamente um marco na teoria administrativa, e representa o primeiro esforço para estabelecer uma relação entre as partes que compõem uma organização e, sobretudo, entre a organização e seu ambiente externo. A abordagem sistémica vê a organização

como um todo integrado, constituída de parte que interagem entre si, e inserida num ambiente com o qual interage permanentemente (LACOMBE & HEILBORN, 2006) citado por Bächtold (2012, 59). Esta teoria considera as organizações como sistemas compostos por interacções dinâmicas entre suas partes e o ambiente externo. Essa visão enfatiza a importância da interdependência dos componentes organizacionais e dos factores externos que influenciam o funcionamento das organizações.

Ainda nesta senda, Chiavenato (2003) enumera três (3) razões que levaram a introdução da teoria de sistemas na teoria administrativa, sendo elas:

1. A necessidade de uma síntese e integração das teorias que a precederam, esforço tentado sem muito sucesso pelas teorias estruturalistas e comportamental;
2. A cibernética permitiu o desenvolvimento e a operacionalização das ideias que convergiam para uma teoria de sistemas aplicadas à administração; e
3. Os resultados bem-sucedidos da aplicação da Teoria de Sistemas nas demais ciências.

Nisto, o sistema pode ser definido como um conjunto de elementos interdependentes que interagem com objectivos comuns formando um todo e onde cada um dos elementos componentes comporta-se, por sua vez, como um sistema cujo resultado é maior do que o resultado que as unidades poderiam ter se funcionassem independentemente. Ou seja, qualquer conjunto pode ser considerado um sistema, desde que as relações entre as partes e o comportamento do todo sejam o foco de atenção (BALLESTERO-ALVAREZ, 1990).

1.5.2.1. Classificação dos sistemas

Os sistemas por sua vez, podem ser fechados ou abertos. A interacção da organização com a sociedade e o ambiente onde ela atua caracteriza essencialmente o chamado sistema aberto.

> Os sistemas abertos envolvem a ideia que determinados inputs são trazidos ao sistema e, processados, geram certos outputs. Com efeito, a organização vale-se de recursos materiais, humanos e tecnológicos, de cujo processamento resultam bens ou serviços a serem fornecidos ao mercado. (BIO, 1998) apud (SILVA et al., 2016).

A organização busca recursos no ambiente, processa-os com ajuda dos recursos internos e devolve ao ambiente, na forma de bens ou serviços. A relação de troca é natural no desenvolvimento de qualquer actividade, assim como a organização busca no fornecedor a

matéria-prima, precisa estar preparada internamente, com recursos humanos e tecnológicos, para transformar essa matéria-prima e devolver à sociedade em forma de produto acabado (SILVA et al., 2016).

Os sistemas abertos trocam energia e informação com seus ambientes e são por eles influenciados.

Figura 01: Sistema aberto

Fonte: CHIAVENATO (2003, 552)

O sistema fechado independe do meio externo para o desenvolvimento das suas funções. Cornachione (1998), afirma que "os sistemas fechados são entendidos como os que não mantêm relação de interdependência com o ambiente externo". Cita-se como exemplo, de sistema fechado o relógio, pois o seu mecanismo trabalha em conjunto, sem precisar do meio externo para o seu funcionamento.

No contexto do e-GOV, o sistema organizacional inclui diversos subsistemas, como os tecnológicos, humanos, administrativos e legais, que devem funcionar harmonicamente para assegurar a prestação de serviços públicos digitais eficientes e seguros. Os ataques cibernéticos representam ameaças que interferem directamente no funcionamento desses subsistemas, impactando a integridade, confidencialidade e disponibilidade das informações e serviços oferecidos pelo e-GOV. De acordo com a teoria de sistemas, um ataque a qualquer parte do sistema pode desestabilizar todo o conjunto, causando falhas e comprometendo os objectivos

organizacionais. Além disso, a teoria destaca que os sistemas são abertos e dependem do ambiente externo para receber insumos, processá-los e devolver resultados. No e-GOV, o ambiente externo inclui factores como ameaças digitais, legislação, infra-estrutura tecnológica e recursos humanos qualificados. Ataques cibernéticos são influências externas negativas que desafiam a capacidade do sistema governamental de se adaptar, responder e se manter funcional.

1.5.3. Quadro conceptual

Embora os detalhes técnicos da segurança cibernética estejam além do escopo deste estudo, os conceitos básicos são essenciais para explicá-lo como um fenómeno sociopolítico.

1.5.3.1. Ataques Cibernéticos

Um ataque cibernético é qualquer esforço intencional para roubar, expor, alterar, desactivar ou destruir dados, aplicações ou outros activos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital.[1] Schneider (2000) refere que os ataques cibernéticos são acções maliciosas realizadas por indivíduos, grupos ou organizações com o objectivo de comprometer, danificar, ou obter acesso não autorizado a sistemas de computador, redes e informações digitais. Esses ataques podem variar desde invasões simples até operações complexas de manipulação de dados ou interrupções em larga escala de serviços online.

No contexto do e-GOV, um ataque cibernético é qualquer acção maliciosa intencional realizada por meio de sistemas digitais e redes de computadores, com o objectivo de comprometer a integridade, confidencialidade ou disponibilidade de dados e serviços públicos prestados online. Esses ataques visam sistemas governamentais como portais de serviços públicos, bases de dados de cidadãos, sistemas fiscais, de saúde, educação, registo civil e até mesmo plataformas eleitorais. Quando bem-sucedidos, podem interromper serviços essenciais, expor dados sensíveis da população, gerar instabilidade institucional e minar a confiança pública no Estado (UNDOC, 2013).

[1] https://www.ibm.com/br-pt/think/topics/cyber-attack

1.5.3.2. Evolução histórica dos ataques cibernéticos

Os primeiros ataques cibernéticos representam os primeiros passos de uma era digital que se desdobraria em uma paisagem virtual complexa e, por vezes, perigosa. Na década de 1970, à medida que os sistemas de computadores se interligaram, as primeiras declarações de ataques cibernéticos emergiram. No entanto, é importante destacar que, nessa época, os motivos foram muitas vezes movidos pela curiosidade e desafio técnico, em vez de objectivos financeiros ou políticos, como são comuns actualmente. Neste contexto, o crime cibernético não é algo pertinente apenas na actualidade, pois desde os tempos arcaicos, cujo meio tecnológico era algo mais longínquo e inacessível para a maioria dos cidadãos, estes já existiam. É necessário compreender que estes crimes começaram a ser praticados ainda na década de 1960, nos Estados Unidos da América (MAIA, COSTA, 2023).

À medida que a tecnologia avançou e a sociedade se tornou cada vez mais dependente da internet, as motivações por trás dos ataques cibernéticos evoluíram consideravelmente. O que antes era um terreno de exploradores digitais e curiosos técnicos se transformou em um campo de actuação para criminosos com uma ampla gama de objectivos, dentre as principais motivações emergentes dos ataques cibernéticos, destacamos as financeiras, políticas, a espionagem cibernética, motivações ideológicas, entretenimento e reconhecimento. Umas das principais motivações para os crimes cibernéticos é o ganho financeiro. Criminosos cibernéticos agora vêem na internet como uma oportunidade de obter lucros substanciais. Isso inclui a realização de fraudes financeiras, como a clonagem de cartões de crédito, a extorsão por meio de *ransomware* e esquemas de *phishing* destinados a roubar informações financeiras de vítimas desavisadas (MAIA, COSTA, 2023a).

A revolução da informação vivenciada pelo mundo contemporâneo é tanto uma bênção quanto uma maldição. É uma maldição porque as TICs têm uma função facilitadora para a perturbação, o crime e a agressão estatal. A dependência das TIC torna-se mais propensa a vulnerabilidades em tempos de agitação social, tensões políticas e outros eventos terríveis. O espectro de ataques cibernéticos é bastante amplo, abrangendo desde actividades individuais a actividades de grupos e atores não estatais, passando por acções governamentais (PAWLAK, 2014).

Quadro 01: Ameaças na infra-estrutura de Tecnologia e Informação do governo electrónico

Categoria	Subcategoria	Exemplos
Integridade Ataques cibernéticos podem usar técnicas de hacking para modificar, destruir ou comprometer a integridade dos dados.	Propaganda/desinformação Modificação ou manipulação de dados ou introdução de dados contraditórios para influenciar um resultado político ou comercial ou desestabilizar um regime estrangeiro	
	Intimidação	Ataques a sites para coagir seus proprietários (públicos ou privados) a remover ou modificar conteúdo, ou seguir algum outro caminho
	Destruição	Destruição permanente de dados para prejudicar concorrentes ou atacar governos estrangeiros. Isso pode, por exemplo, fazer parte de um conflito mais amplo.
Disponibilidade Ataques de negação de serviço por botnets, por exemplo, podem ser usados para impedir que usuários acessem dados que, de outra forma, estariam disponíveis para eles.	Informações externas	Negação de serviço, etc., ataques a serviços governamentais ou privados disponíveis ao público, por exemplo, meios de comunicação, sites de informações governamentais, etc.
	Informações internas	Ataques a intranets privadas ou governamentais, por exemplo, redes de serviços de emergência, infraestrutura de controle de energia e transporte, sites de banco eletrônico, e-mail empresarial, sistemas de comando e controle, etc.
Confidencialidade Ataques cibernéticos podem ter como alvo vários tipos de informações confidenciais, muitas vezes para ganho criminoso.	Espionagem	Empresas que buscam informações sobre seus concorrentes; estados envolvidos em atividades de espionagem (contra estados estrangeiros e indivíduos)
	Roubo de dados pessoais	Ataques de phishing (ou similares) que visam induzir os usuários a revelar dados pessoais, como números de contas bancárias; vírus que registram e carregam esses dados da máquina do usuário
	Roubo de identidade	Cavalos de Tróia, e assim por diante, são usados para roubar informações de identidade que são então usadas na prática de crimes
	Mineração de dados	Técnicas de código aberto empregadas para descobrir, por exemplo, informações pessoais de dados disponíveis publicamente
	Fraude	Frequentemente entregues por e-mail de spam, as fraudes incluem o popular "419" nigeriano ou fraude de taxa antecipada, bem como tentativas de convencer os destinatários a comprar uma variedade de produtos ou serviços fraudulentos.

Fonte: IQBAL, T., & SHAH, S. (2021).

1.5.3.3. Ciberespaço

O ciberespaço é o ambiente virtual criado pelo uso de computadores, redes e a internet, onde pessoas, governos e organizações se comunicam, trocam informações e realizam actividades digitais. É nesse espaço que ocorrem interacções online, como envio de e-mails, transacções bancárias, acesso a serviços públicos (e-GOV), redes sociais, entre outros. Embora seja invisível, o ciberespaço tem impacto real na vida das pessoas e na segurança dos países (FERNANDES, 2012).

Levy (2000) por sua vez, considera-o um espaço de interacção e comunicação entre as pessoas, intermediado pela interconexão das redes de computadores, no qual as informações comunicadas são de natureza digital e as relações desembocam no virtual. Assim, o ciberespaço é todo ambiente digital onde ocorrem as interacções electrónicas entre o governo e os cidadãos, um exemplo claro é quando acessamos um portal electrónico de uma instituição para emitir um documento ou agendar um atendimento.

1.5.3.4. Cibersegurança

A Cibersegurança é o conjunto de medidas que procura garantir o bem-estar e o regular funcionamento da acção de um Estado e das suas populações no ciberespaço e fora dele, desde que derivado de acções directamente a ele acometidas (MILITÃO, 2014, 26). A cibersegurança no contexto do governo electrónico refere-se à protecção de plataformas governamentais digitais e dos dados sensíveis que elas manipulam contra ameaças cibernéticas, como invasões, violações de dados, *malware* e ataques internos, ou seja, são as medidas e ferramentas usadas para proteger os sistemas e dados do governo contra invasões, vazamentos e falhas.

A protecção dos sistemas de governo electrónico é essencial para garantir que os serviços oferecidos sejam confiáveis e fidedignos, e que as informações pessoais dos cidadãos permaneçam protegidas (RAZA, 2024, 115).

Em muitos países africanos, a segurança cibernética não é vista como uma prioridade nacional como nos países desenvolvidos. Isso é enfatizado por Kshetri (2019), que afirma que na África, a segurança cibernética é considerada um luxo e não uma necessidade. Por um lado, países como Maurícia e Tanzânia se destacam como líderes regionais em segurança cibernética. Por outro lado, países como Moçambique, Lesoto e Madagáscar continuam a apresentar níveis mais baixos de compromissos com a segurança cibernética (UIT, 2020).

1.5.3.5. Governo Electrónico

As tecnologias de informação têm acelerado significativamente a transmissão de informações e facilitado a mobilidade do capital. Com os avanços e a redução de custos nos sistemas de transporte e comunicação, o mundo tem-se tornado cada vez mais interconectado, dando a sensação de que está encolhendo. Nesse contexto de profundas transformações, a Administração Pública não poderia permanecer à margem. Um exemplo claro dessa adaptação é o surgimento do projecto de e-GOV, também conhecido como e-governo, que vem sendo implementado em diversos países. O movimento do e-GOV foi formalizado internacionalmente em Janeiro de 1999, quando o então vice-presidente dos Estados Unidos, Al Gore, abriu o 1º Fórum Global sobre Reinvenção do Governo, realizado em Washington, com a participação de representantes de 45 países. Esse evento marcou simbolicamente o início do que se convencionou chamar de e-GOV (HIRSCH, 2003).

O e-GOV seria a utilização da tecnologia de informação e comunicação (particularmente da Internet) para produzir e distribuir serviços públicos de modo mais conveniente do que a maneira tradicional, tornando-se mais orientada ao cliente, com melhor relação custo-benefício, de forma diferenciada e melhor, o e-GOV afectaria o modo como a organização pública se relaciona com cidadãos, empresas e outras instituições, assim como seus processos internos e a relação com servidores (HOLMES, 2001).

Usando a definição de (ZWEERS, PLANQUÉ, 2003), pode-se dizer que governo electrónico é um conceito emergente que objectiva fornecer ou tornar disponível informações, serviços ou produtos, por meio electrónico, a partir ou através de órgãos públicos, a qualquer momento, local e cidadão, de modo a agregar valor a todos os stakeholders envolvidos com a esfera pública.

Para o Banco Mundial apud (FERNANDO, 2016):

> O e-Gov refere-se à utilização por órgãos governamentais de Tecnologias de Informação (como *Wide Area Networks*, a Internet, e computação móvel), que têm a capacidade de transformar as relações com os cidadãos, empresas e outros ramos do governo. Essas tecnologias podem servir uma variedade de diferentes fins: uma melhor prestação de serviços do governo para cidadãos, melhores interacções com empresas e indústrias, empoderamento dos cidadãos por meio do acesso à informação, ou a gestão do governo

> mais eficiente. Os benefícios resultantes podem ser menos corrupção, maior transparência, maior comodidade, o crescimento da receita, e/ou redução de custos.

Desse modo, o governo electrónico pode ser visto como um conceito que envolve bem mais do que a simples ideia de um "governo informatizado". Tratasse de um governo aberto e ágil para melhor atender à sociedade. Deve utilizar as tecnologias da informação e de comunicação para ampliar a cidadania, aumentar a transparência da gestão e a própria participação dos cidadãos na fiscalização do poder público, além de democratizar o acesso aos meios electrónicos, explica (CHAHIN, 2004).

A ideia de governação electrónica surge de forma a alcançar o objectivo de democratizar os governos e haver maior transparência e controle social. O governo electrónico veio reduzir os gastos da administração pública e melhorar a utilização dos recursos, pois muitos serviços passam a ser realizados por meio electrónico pela própria sociedade e a qualquer hora, gerando diminuição no número de servidores e/ou terceirizados que até então realizavam actividades burocráticas, desse modo, o governo electrónico revela-se mais eficiente do que o governo tradicional nas suas administrações (VIEIRA & SANTOS, 2010).

Ao aumentar a transparência, reduzir a burocracia e fornecer acesso à informação em tempo real, os sistemas de governo electrónico têm o potencial de aumentar significativamente a eficiência e a eficácia da administração pública (KHAN apud RAZA, 2024).

À medida que governos em todo o mundo adoptam cada vez mais plataformas digitais para fornecer serviços públicos, tornam-se mais vulneráveis a uma série de ameaças cibernéticas. Com o surgimento de serviços *online,* identidades digitais e a interconexão dos sistemas governamentais, as plataformas de governo electrónico estão sendo alvos cada vez mais frequentes de cibercriminosos. A crescente sofisticação dos ciberataques, aliada à evolução de ameaças como *ransomware, phishing* e ataques *DDoS*, representam desafios significativos para a segurança dessas plataformas. O ritmo acelerado das mudanças tecnológicas e a complexidade das questões de segurança cibernética frequentemente superam as capacidades dos sistemas de tecnologia de informação governamentais, tornando cada vez mais difícil a defesa eficaz contra ameaças cibernéticas (IQBAL, SHAH, 2021, 80)

Para que os sistemas de governo electrónico sejam eficazes, eles devem ser percebidos como seguros e confiáveis pelos cidadãos e pelas partes interessadas. Quando ocorrem violações de segurança cibernética, a confiança pública na governança digital pode ser severamente prejudicada.

Jameel e Rizvi (2020) referem que a falta de confiança na capacidade dos governos de proteger dados sensíveis pode levar à redução da participação dos cidadãos nos serviços de governo electrónico, prejudicando assim a eficácia geral das iniciativas de governança digital. Garantir mecanismos robustos de segurança cibernética é, portanto, crucial não apenas para a integridade operacional dos serviços de governo electrónico, mas também para manter a confiança do público na transformação digital dos serviços públicos.

Foi tendo como base nas maiores vantagens das tecnologias de informação e comunicação que a política de informática de Moçambique definiu, como um dos seus objectivos estratégicos de implementação, criação de uma rede electrónica de todos os órgãos e departamentos centrais do governo e dos governos provinciais e outras estruturas do Estado. A criação da rede electrónica leva à implantação, na administração pública moçambicana, do governo electrónico. O Governo electrónico traduz uma administração pública baseada nos equipamentos tecnológico no processo de prestação de serviços públicos aos cidadãos. O desafio de governo, no contexto electrónico, é o de prestação de serviços públicos de qualidade (JOÃO, 2023).

1.5.3.6. Estágio do governo electrónico e suas características

De acordo com Heywood (2013) apud (FERNANDO, 2016, 29), o governo electrónico não é um processo de uma única etapa e nem pode ser implementado como se fosse um único projecto. O governo electrónico é de natureza evolutiva e envolve várias etapas ou fases de desenvolvimento. Vários são os modelos usados na avaliação dos estágios do governo electrónico no mundo, muitos dos quais com inúmeras similaridades, o que dispensa a sua apresentação exaustiva. Assim, para Viana (2021, 120) o governo electrónico é dividido pelas seguintes fases ou etapas:

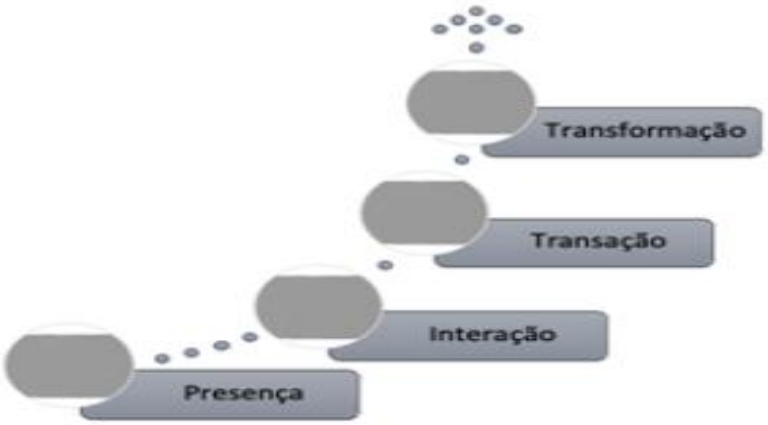
I. A primeira, *a presencial ou informacional*, corresponde na mais básica. É quando uma determinada instituição cria uma página na internet e traz algumas informações. Aqui, o governo ainda atende principalmente presencialmente, mas já começa a disponibilizar informações básicas *online*.

II. A segunda fase é a da *interacção*, em que serviços passam a ser prestados. Há ferramentas de busca, *downloads* de arquivos e formulários. Esta etapa inclui capacidades informativas e apresenta formas simples de navegação, exploração e interacção com dados. Nesta fase, os cidadãos já começam a interagir com o governo pela internet, como preencher formulários online, enviar e-mail, agendar atendimentos, porém, ainda precisa ir presencialmente para finalizar o serviço.

III. A terceira etapa, a de *transação*, corresponde na interacção entre governo e cidadão. Aqui, as capacidades transaccionais conduzem transacções *online* completas por meio de comunicação segura, e muitas vezes em tempo real. O serviço público já pode ser realizado completamente online, sem precisar ir até um órgão público;

IV. Finalmente, a quarta etapa, chamada de *transformação*, traz uma conexão substancial entre cidadãos e governo, que ocorre quando há uma integração completa dos sistemas. Isto é, há uma troca de informações entre as diversas entidades governamentais. Distintamente da fase de transacção em que se tem um único sistema, na etapa da transformação os sistemas estão interligados. Denota-se uma conexão rápida entre órgãos, instituições e atores, correspondendo numa configuração "holística" da administração que se coloca inteiramente digitalizada e interconectada.

Figura 02: etapas da transformação digital no e-GOV



Fonte: Viana (2021, 120)

Ainda segundo a mesma autora, essas fases são por vezes identificadas de acordo com o grau de avanço de um determinado governo na implementação do governo electrónico. Elas podem

também se referir à década de surgimento das tecnologias. De um modo ou de outro, são úteis e servem para identificar o estágio de evolução de um governo electrónico. As Nações Unidas empregam essas etapas como modo de identificação do avanço no desenvolvimento da transformação digital de um dado país.

1.5.3.7. Potencial do governo electrónico

Através da aplicação das TICs e da modernização da Administração Pública, as medidas relacionadas com a implementação do e-GOV podem proporcionar, se correctamente aplicadas, importantes melhorias em múltiplas vertentes, tais como (ALVES, MOREIRA, 2004):

- Simplificação da prestação de muitos serviços aos cidadãos e às empresas, com especial incidência naqueles onde o tratamento de documentos e o processamento de informação assume grande relevância;
- Maior rapidez e facilidade na obtenção de informação e no esclarecimento de dúvidas por parte dos cidadãos e das empresas relativamente à Administração Pública;
- Elevação dos padrões de eficiência e redução dos custos da Administração Pública, com potencial eliminação de níveis supérfluos de gestão e integração de sistemas e serviços sempre que possível;
- Aumentar a capacidade de resposta da Administração Pública às iniciativas dos cidadãos e proporcionar-lhes possibilidades de participação mais alargada;
- Colaboração mais próxima entre os vários níveis do Estado e os vários serviços da Administração Pública, evitando redundâncias, optimizando recursos e promovendo uma mais eficaz aplicação do princípio da subsidiariedade

1.5.3.8. Estratégia do Governo Electrónico em Moçambique

Em Moçambique, a Estratégia de Governo Electrónico, implantada a partir do Programa Quinquenal do Governo (2005-2009), levou à criação do Governo Electrónico (e-Gov) em 2011. De acordo com o documento oficial da Estratégia de Governo Electrónico de Moçambique (MOÇAMBIQUE, 2005), os principais objectivos gerais dessa iniciativa são:

a) Melhorar a eficiência e a eficácia na prestação de serviços públicos, por meio da utilização de ferramentas digitais que tornam os processos mais rápidos e acessíveis;

b) Assegurar a transparência e a responsabilidade dos servidores públicos, através da digitalização dos processos administrativos, que facilita o controlo e a prestação de contas;
c) Facilitar o acesso à informação, aprimorando as actividades do sector privado e simplificando a vida dos cidadãos, ao tornar mais acessíveis serviços e dados importantes para o desenvolvimento social e económico.

Enquadrada no âmbito da Estratégia Global da Reforma do Sector Público (EGRSP), a política de governo electrónico de Moçambique foi desenhada especificamente para apoiar a terceira fase dessa reforma, programada para o período 1990-2011. Nesse período, concretamente a partir de 2006, ano da sua criação, o governo electrónico de Moçambique ganhou reconhecimento e aceitação crescentes na prática da governação, ficando "o seu maior ou menor impacto a depender do maior ou menor grau de integração transversal nas políticas, estratégias e programas dos governos assim como dos recursos disponibilizados para a sua materialização." (MOÇAMBIQUE- ESTRATÉGIA DO GOVERNO ELETRÔNICO, 2010, p. 1)

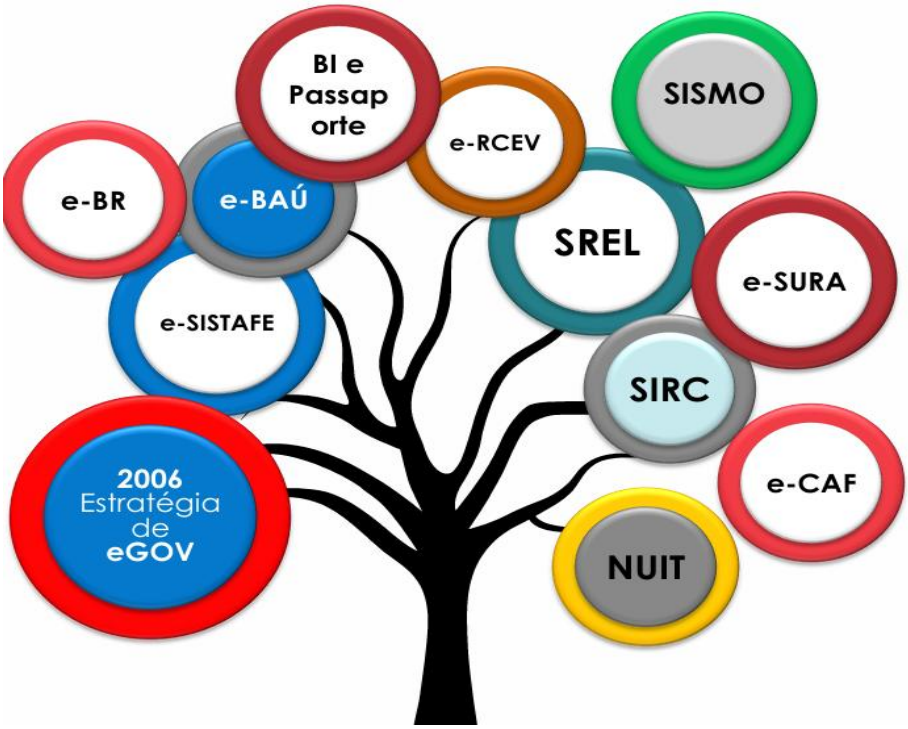


Figura 03: Serviços oferecidos pelo e-GOV desde sua adopção em 2006

A Estratégia de Implementação do Governo Electrónico defende acesso generalizado às Tecnologias de Informação e Comunicação pretendendo que este seja do alcance de todas as pessoas o que significa que enquanto o governo estiver disponível e disponibilizado, electronicamente, (através de páginas de internet, email, contactos telefónicos para chamadas ou SMS e outras formas do governo electrónico), o povo (as pessoas), poderá beneficiar mais efectivamente, dos seus serviços e quiçá, participar da sua governação (FERNANDO, 2023, 27-28). Conforme apresentado pelo Gabinete da Estratégia de e-GOV,

> a política de governo electrónico de Moçambique é, nesta era da informação, o instrumento mais adequado para a colocação dos serviços públicos ao alcance do cidadão a qualquer momento e em qualquer lugar, para uma prestação de serviços mais eficaz e eficiente e menos dispendiosa, e para a redução da burocracia e oportunidades de corrupção. (MOÇAMBIQUE ESTRATEGIA GOVERNO ELETRÔNICO, 2005).

Assim, a Estratégia de Governo Electrónico em Moçambique não é apenas uma ferramenta tecnológica, mas também um caminho para melhorar a participação dos cidadãos, diminuir a burocracia e tornar a gestão pública mais transparente. No entanto, para que funcione plenamente, ainda é preciso enfrentar dificuldades ligadas à infra-estrutura, à tecnologia e à formação de pessoas, o que mostra a importância de políticas sólidas de cibersegurança e de investimentos contínuos no sector digital.

CAPITULO II: REVISÃO DE LITERATURA

2. Tipos de ataques cibernéticos que afectam o e-GOV

Os sistemas de governo electrónico, devido ao seu amplo acesso e natureza crítica, enfrentam inúmeras ameaças à segurança cibernética. À medida que os governos adoptam plataformas digitais mais avançadas, eles se expõem a diversas formas de ataques cibernéticos que podem comprometer os serviços públicos, a integridade dos dados e a privacidade dos cidadãos. Alguns dos tipos mais comuns e significativos de ameaças à segurança cibernética que visam sistemas de governo electrónico segundo Raza (2024, 130) são:

- ***Malware e Ransomware***

O *malware* é um programa malicioso criado para invadir, danificar ou espionar computadores e sistemas. Ele pode ser usado para roubar informações importantes, como dados de cidadãos, documentos sigilosos e até senhas. Já o *ransomware* é um tipo de *malware* ainda mais perigoso, ele bloqueia o acesso aos sistemas e arquivos e só libera mediante o pagamento de um resgate geralmente cobrado em moedas digitais, que dificultam a identificação dos criminosos (BRASIL, 2021).

Órgãos públicos são alvos estratégicos para esses ataques, principalmente por centralizarem grandes volumes de dados sensíveis e operarem sistemas que afectam directamente a população, como saúde, segurança, justiça e arrecadação fiscal. Além disso, a falta de investimentos em infra-estrutura de tecnologia, políticas de segurança da informação e capacitação técnica agrava a vulnerabilidade dessas instituições (OLIVEIRA; FREITAS, 2020).

- **Phishing e Engenharia Social**

No cenário actual de digitalização dos serviços públicos, o e-GOV tem permitido que a população acesse informações, solicite documentos e realize serviços de forma mais ágil e prática, sem precisar sair de casa. No entanto, essa modernização também abriu espaço para novas formas de crimes digitais, como o *phishing* e a engenharia social, que representam sérios desafios para a administração pública (BRASIL, 2021).

Phishing é uma técnica usada por criminosos para enganar usuários e induzi-los a fornecer informações confidenciais, como senhas, dados bancários ou de acesso a sistemas públicos. Isso

geralmente é feito por meio de mensagens falsas enviadas por e-mail, SMS ou redes sociais que imitam comunicações oficiais de órgãos do governo. Muitas vezes, esses ataques direccionam o cidadão para páginas falsas que se parecem com os portais oficiais, levando-o a inserir seus dados sem perceber o golpe (BRASIL, 2021).

Já a engenharia social é um conjunto de estratégias que exploram o comportamento humano, ou seja, a tendência natural das pessoas de confiar ou agir por impulso. Ao invés de atacar directamente os sistemas, os criminosos atacam os próprios usuários sejam cidadãos ou servidores públicos persuadindo-os a clicar em links maliciosos, abrir arquivos infectados ou divulgar informações sensíveis. Em ambientes públicos, isso pode ocorrer por meio de telefonemas, mensagens ou até conversas presenciais (OLIVEIRA, FREITAS, 2020, 234).

- **Negação de Serviço (DoS) e Negação de Serviço Distribuída (DDoS)**

Os ataques de DoS ocorrem quando um sistema é sobrecarregado com um volume anormal de acessos, impedindo que usuários legítimos consigam utilizar os serviços. Já os ataques de DDoS funcionam da mesma forma, porém são ainda mais potentes por envolverem vários computadores ao mesmo tempo, espalhados em diferentes locais, todos controlados por um invasor. O objectivo é o mesmo: tornar os serviços indisponíveis (BRASIL, 2021).

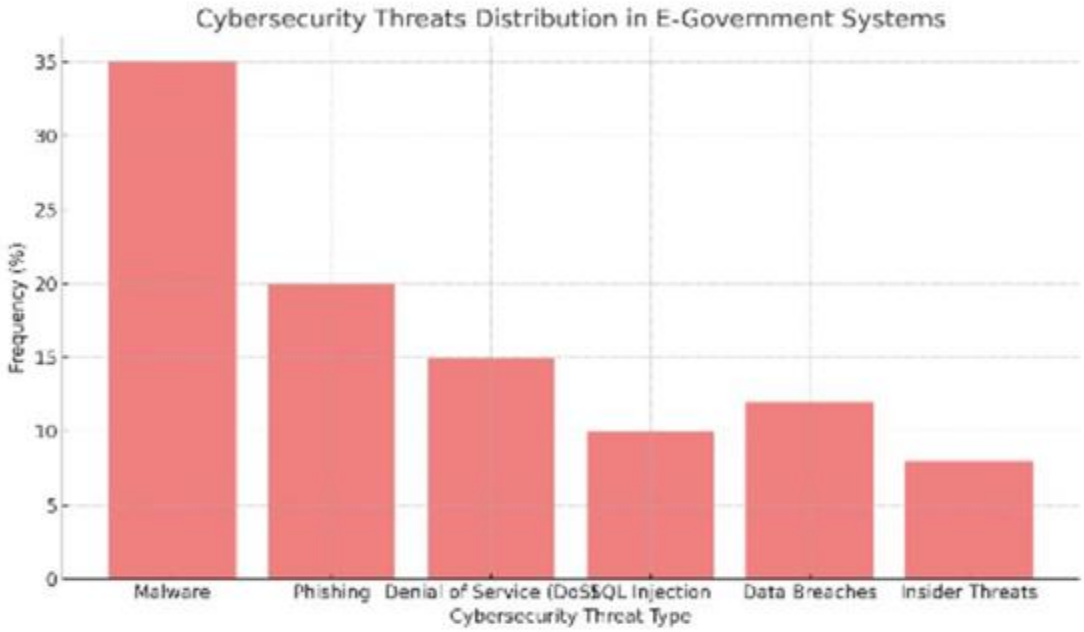
Para Oliveira e Freitas (2020), no contexto da Administração Pública, isso pode significar, por exemplo, que um cidadão não consiga acessar o portal de uma dada instituição pública, emitir documentos ou fazer agendamentos, quando esses serviços são interrompidos, a credibilidade do poder público é afectada, gerando insatisfação, atrasos e prejuízos.

Um ataque DDoS não necessariamente rouba dados ou acessa sistemas internos, mas seu impacto é grave porque afecta directamente a disponibilidade, que é um dos pilares da segurança da informação no sector público. Além disso, em períodos críticos como datas de declaração do Imposto de Renda ou processos selectivos a sobrecarga provocada por um DDoS pode paralisar completamente os serviços digitais de um órgão. Esses ataques têm se tornado cada vez mais comuns, por serem relativamente fáceis de executar e difíceis de rastrear. Eles podem ser motivados por interesses políticos, tentativas de chantagem, activismo digital ou simplesmente para causar instabilidade em momentos estratégicos da gestão pública (Idem, 2020).

- **Ameaças internas**

Ameaças internas envolvem indivíduos dentro do sistema governamental que, intencionalmente ou não, fazem mau uso de seu acesso a dados e sistemas confidenciais para fins maliciosos. Esses insiders podem incluir funcionários públicos, contratados ou fornecedores terceirizados que têm acesso a infra-estrutura crítica. Ameaças internas são particularmente preocupantes porque esses atores já têm acesso autorizado ao sistema, tornando suas acções difíceis de detectar (RAZA: 2024).

Gráfico 01: Distribuição de ameaças à segurança cibernética em sistemas de governo na última década



Fonte: Raza (2024, 140)

O *malware* (ou vírus de software) figura como o ataque mais recorrente contra os sistemas governamentais, isto deve-se ao facto deste ser mais difícil de rastrear, e quando a instituição está sob esses ataques, caso esta não tenha um sistema de cibersegurança, dificilmente notará. Vários *hackers* injectam vírus nos sistemas governamentais de variadas formas para poder ter o controlo e por conseguinte poder extrair as informações por estes desejados.

2.1. Factores que tornam o e-Gov vulnerável aos ataques cibernéticos

O cibercrime está presente nos países desenvolvidos e não só. De facto, o funcionamento do e-GOV assenta em estruturas de telecomunicações e sistemas de informação susceptíveis de sofrerem ataques a partir de um número infindável de localizações e com meios relativamente mais acessíveis do que sucedia no passado (ALVES, MOREIRA, 2004, 25-26). Os mesmos autores indicam que¸ interdependência acarreta uma complicação adicional, uma vez que a ligação estreita entre os vários sistemas implica que qualquer ataque bem-sucedido a um deles se poderá transmitir em cascata a todo o aparelho do Estado, amplificando as consequências negativas. Este risco é especialmente importante numa conjuntura internacional de grande instabilidade e em que a ameaça de organizações terroristas transnacionais está cada vez mais presente.

Os autores Rashid e Saeed (2022) apud (RAZA, 2024, 140) avançam que os sistemas de e-GOV estão expostos a diversas vulnerabilidades que podem comprometer significativamente sua segurança. Essas vulnerabilidades decorrem de factores tecnológicos e humanos e podem deixar redes, serviços e dados governamentais susceptíveis a ataques cibernéticos, os seguintes factores tornam o e-GOV vulnerável aos ataques cibernéticos:

- **Sistemas Ligados e Protocolos de Segurança Inadequados**

Uma das principais vulnerabilidades em sistemas de governo electrónico é a dependência contínua de infra-estruturas de tecnologia de informação conectadas, que muitas vezes carecem de actualizações de segurança modernas. Organizações governamentais ainda utilizam plataformas de *hardware* e *software* obsoletas, mais propensas a ataques cibernéticos, pois não recebem actualizações regulares nem suportam protocolos de segurança avançados (RASHID e SAEED, 2022). Esses sistemas antigos frequentemente apresentam falhas de segurança conhecidas, que não foram corrigidas, tornando-se alvos fáceis para criminosos digitais.

Segundo Raza (2024), essa situação é agravada pelo facto de que a maioria desses sistemas legados não fora desenvolvida com foco nas ameaças cibernéticas modernas, o que os torna ainda mais vulneráveis à medida que a complexidade dos ataques aumenta. Além disso, como ressalta o autor, a conectividade constante desses sistemas à internet, sem defesas adequadas,

amplia consideravelmente a superfície de ataque, facilitando a acção de *malwares*, acessos não autorizados e violações de dados.

- **Falta sensibilização sobre segurança cibernética entre funcionários do governo**

A eficácia das medidas de segurança cibernética em sistemas de e-GOV é frequentemente prejudicada pela falta de sensibilização entre os funcionários públicos sobre ameaças digitais e as formas adequadas de mitigá-las. Funcionários podem, mesmo sem intenção, comprometer a segurança dos sistemas ao se tornarem vítimas de ataques de *phishing*, ao gerenciar senhas de forma inadequada ou ao não reconhecer comportamentos suspeitos em suas actividades rotineiras (RAZA, 2024). A ausência de uma cultura institucional de segurança digital é um dos principais factores de risco no sector público, já que muitos servidores não possuem formação técnica suficiente para identificar ameaças como tácticas de engenharia social, isso pode facilitar o acesso não autorizado a sistemas governamentais por meio da exploração do erro humano (idem, 2024).

Nesse sentido, os governos devem investir continuamente em programas de capacitação e treinamento em segurança cibernética, destinados a todos os níveis da administração. Esses programas devem abordar desde o gerenciamento seguro de senhas até o uso consciente do e-mail e das redes digitais institucionais.

- **Mecanismos de autenticação fracos**

Mecanismos de autenticação fracos representam outra vulnerabilidade significativa nos sistemas de governo electrónico. Muitas plataformas públicas ainda utilizam protocolos simples baseados apenas em senhas, os quais são especialmente vulneráveis a ataques como força bruta, preenchimento de credenciais e *phishing*. Segundo Raza (2024), a dependência exclusiva de autenticação por senha, sem o uso de mecanismos adicionais como autenticação multifactor, representa um risco elevado, sobretudo em ambientes governamentais que processam informações sensíveis.

Outro factor agravante, conforme também apontado pelo autor citado acima, é a prática comum entre funcionários públicos e cidadãos de utilizar senhas fracas, repetidas ou padrões fáceis de adivinhar, o que compromete seriamente a eficácia dos controles de segurança implementados. Sem uma política robusta de autenticação e criptografia, sistemas públicos continuam vulneráveis, mesmo com investimentos em infra-estrutura tecnológica.

2.2. Consequências dos ataques cibernéticos no governo electrónico

As consequências dos ataques cibernéticos no e-GOV têm se tornado um tema de crescente relevância, especialmente diante da ampliação da digitalização dos serviços públicos e da dependência das tecnologias da informação para a prestação de serviços à população. Entre os principais impactos, destaca-se o prejuízo à confiança do cidadão nas instituições governamentais. Ataques cibernéticos recorrentes podem levar a uma percepção generalizada de vulnerabilidade e ineficácia por parte do Estado. Conforme destaca Guedes (2018), essa percepção de insegurança pode resultar na diminuição da participação cidadã e na menor adesão aos serviços digitais, minando os avanços conquistados pela administração pública na oferta de serviços por meios electrónicos.

Outro efeito crítico desses ataques é a exposição de dados sensíveis, sobretudo informações pessoais dos cidadãos. Alves e Moreira (2004) ressaltam que a violação de dados pode gerar consequências graves, como fraudes, roubo de identidade e outros crimes que afectam directamente a segurança individual. Além disso, tais incidentes podem acarretar repercussões legais e financeiras significativas para o Estado, inclusive em termos de responsabilidade civil e administrativa, caso falhas de protecção sejam comprovadas.

No campo económico, os ataques cibernéticos também têm impacto expressivo. O relatório *Cost of Cybercrime*, realizado pela Accenture (2019), estima que o custo global das acções criminosas na esfera digital atinge trilhões de dólares por ano, considerando não apenas os custos directos com recuperação de dados e sistemas, mas também perdas relacionadas à produtividade, imagem institucional e credibilidade. Nessa mesma linha, Saxena (2013) argumenta que a investigação, mitigação e recuperação de ataques exigem grandes investimentos públicos, além da possibilidade de indemnizações às vítimas e o enfrentamento de responsabilidades legais

complexas. Por fim, os ataques cibernéticos podem resultar em desestabilização dos serviços públicos, especialmente aqueles considerados essenciais.

Em sua obra *Understanding Privacy*, Solove (2008) afirma que a interrupção de serviços digitais compromete a capacidade do governo de executar suas funções básicas, colocando em risco tanto a segurança pública quanto o bem-estar social. Esse tipo de crime, no contexto da governança electrónica, afecta directamente a acessibilidade dos cidadãos a informações importantes e à execução de transacções fundamentais, como emissão de documentos, acesso à saúde ou regularização fiscal. Complementando esse raciocínio, Saxena (2023) destaca que a interrupção de tais serviços compromete não apenas o funcionamento da máquina pública, mas também os direitos básicos do cidadão no ambiente digital.

2.3. Desafios no combate aos ataques cibernéticos

Os desafios mais significativos que os países em vias de desenvolvimento enfrentam na área de cibersegurança são semelhantes aos enfrentados por outras nações dos Balcãs Ocidentais. De acordo com o autor Segundo (2015), uma questão urgente é a falta de normas e regulamentações adequadas, bem como a ausência de conscientização pública sobre o tema, o que contribui para a criação de um ambiente vulnerável à violência cibernética. Outra preocupação recorrente está relacionada à preservação de informações confidenciais.

Dados e informações oficiais sensíveis, que estão sob constante risco de ataques cibernéticos, frequentemente não são protegidos por sistemas de segurança da informação eficazes. Além disso, temas como privacidade de dados e disseminação de notícias falsas vêm sendo apontados como factores adicionais que, de forma relativamente recente, têm causado confusão e desinformação na sociedade (ASLLANI, 2022).

A baixa notificação de violações também representa um obstáculo importante. Isso ocorre por diversos motivos, entre os quais o temor das instituições públicas de que a divulgação de incidentes envolvendo dados de seus usuários resulte em perdas de credibilidade. Por essa razão, muitas preferem manter tais informações ocultas. O autor refere ainda que a eficiência da defesa do ciberespaço é limitada por falta de recursos, orçamentos reduzidos, instituições pouco

capacitadas e escassez de profissionais especializados, o que compromete a implementação de políticas de segurança cibernética consistentes.

Outro problema relevante é o baixo investimento governamental em segurança da informação, que concorre com outras áreas consideradas mais prioritárias. Além disso, há uma ausência de legislação específica ou actualizada sobre crimes cibernéticos, protecção de dados e responsabilidade digital, o que dificulta a actuação jurídica do Estado na investigação, punição e cooperação internacional em casos de ataques complexos (SAXENA, 2023).

A fragmentação entre órgãos públicos também compromete a eficácia da resposta estatal. Muitas instituições não compartilham informações de forma integrada, o que dificulta uma resposta coordenada a ameaças que afectam múltiplos sectores simultaneamente. Por fim, destaca-se ainda que a maioria dos servidores públicos não recebe treinamento adequado em segurança digital, o que eleva os riscos de ataques simples, como *phishing*, roubo de credenciais e violações causadas por erro humano (idem, 2023).

Os ataques cibernéticos ao governo electrónico representam uma das maiores ameaças à administração pública contemporânea. Conforme exposto, tais ataques podem assumir diferentes formas desde *malware* e *phishing* até ataques de negação de serviço e ameaças internas, explorando fragilidades tecnológicas e humanas. As consequências vão além da interrupção de serviços, atingindo a confiança dos cidadãos, a privacidade dos dados pessoais, a credibilidade das instituições e a estabilidade económica.

Fica evidente que a vulnerabilidade do e-GOV resulta não apenas de limitações técnicas, como sistemas obsoletos e mecanismos de autenticação frágeis, mas também da ausência de uma cultura institucional de segurança digital entre servidores públicos. Do mesmo modo, a falta de legislação adequada, de recursos financeiros e de profissionais especializados agrava a dificuldade de enfrentar esse fenómeno em países em desenvolvimento, como o caso de Moçambique.

CAPITULO III: METODOLOGIA DE TRABALHO

3. Metodologia

Metodologia é a aplicação de métodos e procedimentos que auxiliarão na observação, na aplicação, na colecta de dados, para que se chegue a um resultado, e/ou a comprovação, podendo ser utilizada em diversas categorias da sociedade (ALMEIDA, 2021).

3.1. Natureza da pesquisa

Quanto a natureza, esta pesquisa é básica¸ segundo Almeida (2021) esta visa o progresso da ciência com o intuito de adquirir novos conhecimentos científicos, não se preocupando com a sua aplicação prática, sendo generalista, buscando construir principalmente teorias e lei. Para Gil (2002), a pesquisa básica aglutina estudos que tem como objectivo completar uma lacuna no conhecimento e gerar conhecimento novo para o avanço da ciência. Esta pesquisa busca gerar verdades, ainda que temporárias e relativas, de interesses mais amplos, não localizados não tendo, todavia, o compromisso de aplicação prática do resultado.

Após a realização da pesquisa espera-se dar um contributo na questão ligada a conscientização sobre os ataques cibernéticos no e-GOV e tecer algumas recomendações para a sua melhoria.

3.2. Quanto a abordagem

Quanto a abordagem¸ a pesquisa é qualitativa. Para Almeida (2021)¸ a pesquisa qualitativa considera a interpretação dos fenómenos e as relações com inúmeros significados, além disso, um vínculo entre o mundo objectivo e o sujeito. Não necessita de usos estatísticos e matemáticos, tendo o ambiente como fonte de colecta de dados, com descrição do estudo. Então, podemos afirmar que a pesquisa qualitativa se baseia na natureza e na essência dos fenómenos, utilizando-se do trabalho de campo, da etnografia, subjectivismo e naturalismo.

De acordo com Trivinos (1987), a abordagem qualitativa trabalha os dados buscando seu significado, tendo como base a percepção do fenómeno dentro do seu contexto. O uso da descrição qualitativa procura captar não só a aparência do fenómeno como também suas essências, procurando explicar sua origem, relações e mudanças, tentando intuir as consequências.

Os ataques cibernéticos têm vindo a ganhar espaço na sociedade moçambicana assim como no Estado, a sua análise é importante para entender às repercussões que estes ataques podem causar assim como para adoptar estratégias de combate.

3.3. Objectivos da Pesquisa

Quanto ao objectivo está pesquisa tem um carácter descritivo, pois encontra-se vinculada, apenas à descrição e registo de factos sem a intervenção sobre eles, ou seja, descreve, regista, observa, analisa e relaciona os dados das características de um grupo social, de uma população, de um fenómeno, ou sobre as relações existentes no estudo. Questionários, formulários, entrevistas, a observação sistemática, entre outros, são bastante utilizadas como colecta de dados, sendo este tipo de método de colecta conhecido como levantamento (PRODANOV e FREITAS, 2013).

Deste modo, iremos descrever, explicar e interpretar o fenómeno dos ataques cibernéticos no governo electrónico no Instituto Nacional de Tecnologias de Informação e Comunicação que é objecto do estudo.

3.4. Tratamento do procedimento técnico

Para o presente estudo, é aplicado o método monográfico ou estudo de Caso. O Método monográfico ou estudo de caso, de acordo com Gil (2002, 54), consiste no estudo profundo e exaustivo de um ou poucos objectos, de maneira que permita seu amplo e detalhado conhecimento e para a realização da pesquisa. Nestes termos, pautou-se por situações da vida real (institucional), possibilitando assim, a descrição do problema no contexto em que está sendo feita a pesquisa. Vincula-se a pesquisa Aplicada, de ordem prática, para solucionar um problema social que consiste em colectar informações sobre um determinado indivíduo, grupo, comunidade, entre outros, podendo ser utilizado tanto em pesquisas exploratórias, descritivas e explicativas (ALMEIDA, 2021).

Esse método de procedimento, enquadra-se melhor na nossa pesquisa, visto que analisa os ataques cibernéticos no governo electrónico.

3.5. Técnica de recolha de dados

Em primeiro lugar, é preciso lembrar que método e técnica designam realidades diferentes. Soriano (2004), afirma que o método representa como se pesquisa, enquanto a técnica representa por meio de que se pesquisa. O autor ainda acrescenta um terceiro elemento, o instrumento de pesquisa, que seria o meio físico para se pesquisar (como por exemplo um guião de observação ou um roteiro de entrevista).

Quanto aos procedimentos técnicos, optou-se pela Pesquisa Bibliográfica, Documental e Entrevista semiestruturada.

- **Pesquisa bibliográfica**

Elaborada a partir de materiais já publicados, como por exemplo: livros, revistas, jornais, panfletos, monografias, artigos científicos, dissertações, teses, material cartográfico, publicações em periódicos, internet; onde o pesquisador vai entrar em contacto com materiais que contém informações sobre um determinado conteúdo de sua pesquisa. É de extrema importância que o pesquisador verifique a verossímidade das informações de sua fonte de dados. Praticamente, todas as pesquisas necessitam de um estudo bibliográfico para embasar seus projectos de pesquisa (BELLO, 2009).

- **Pesquisa Documental**

Pesquisa documental, por sua vez, serviu de base para a recolha de informação relevante para o estudo recorrendo a leitura de alguns documentos oficiais (Legislação, Estratégias e outros) existentes sobre o tema (FONSECA, 2002).

Neste recorremos aos relatórios, avaliações e programas relacionados ao INTIC.

- **Entrevista**

A entrevista constitui uma série de perguntas que consiste na comunicação bilateral. Na presente pesquisa, optou-se pela entrevista de carácter exploratório, onde foram usadas eventuais indagações ou levantamento de dados e informações que não estavam contempladas no formulário (KAUARK et al., 2010). Para facilitar a colecta de dados sobre o tema em questão, adoptou-se a entrevista semiestruturada, na qual o entrevistador prepara uma lista padronizada de perguntas, mas acrescenta, em cada entrevista conduzida, perguntas adicionais que permitam

maior alcance dos objectivos, de acordo com os comentários e respostas do entrevistado. Essa abordagem confere maior liberdade e flexibilidade ao entrevistador, possibilitando o aprofundamento e esclarecimento das respostas (MAY, 2004).

Dencker (2000) destaca que a entrevista permite maior flexibilidade na elaboração das questões e promove maior sinceridade por parte do respondente.

A entrevista foi realizada entre os meses de Abril e Agosto de 2025. Para isso, utilizou-se um guia de entrevistas contendo perguntas específicas sobre a análise dos ataques cibernéticos no governo electrónico no período de 2020 a 2023, com foco no Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC). As informações recolhidas foram registadas em bloco de notas para posterior análise.

A amostra da população seleccionada para a realização das entrevistas foi composta por dois participantes-chave, representantes de instituições envolvidas directamente com a gestão e segurança da informação no sector público. A primeira entrevista foi realizada no INAGE, cujo entrevistado será identificado como "E1". A segunda entrevista ocorreu nas instalações do INTIC, com duração média entre 30 e 40 minutos, sendo o entrevistado designado como "E2" ao longo da análise dos dados. A escolha desses participantes baseou-se em sua experiência e conhecimento específico sobre o tema investigado, garantindo a relevância e a profundidade das informações colectadas para a pesquisa.

3.6. Técnicas de análise de conteúdo

A análise de conteúdo é um conjunto de técnicas de investigação qualitativa voltadas à identificação, interpretação e extracção de significados de materiais comunicativos. Segundo Campos (2004), trata-se da busca pelo sentido ou pelos múltiplos sentidos contidos em um documento. Para Bardin (2011), a análise de conteúdo consiste em um conjunto de procedimentos sistemáticos e objectivos de descrição do conteúdo das mensagens, permitindo a realização de inferências válidas e replicáveis a partir de dados textuais. Essa técnica oferece ao pesquisador a possibilidade de identificar significados explícitos ou implícitos em diferentes tipos de materiais, tais como entrevistas, documentos institucionais, reportagens, discursos políticos, programas de televisão, postagens em redes sociais, entre outros.

No contexto desta pesquisa, a análise de conteúdo foi aplicada a documentos oficiais do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), bem como a artigos científicos, monografias e entrevistas realizadas com profissionais das instituições envolvidas. A adopção dessa técnica permitiu uma leitura crítica e aprofundada do material empírico e teórico, contribuindo para a compreensão dos ataques cibernéticos no âmbito do governo electrónico.

3.7. Limitações

Durante a realização da pesquisa, enfrentaram-se três principais limitações. A primeira foi a dificuldade de enquadrar o tema dos ataques cibernéticos no campo da Administração Pública, pois trata-se de uma temática tradicionalmente abordada sob a óptica da informática ou das engenharias, o que exigiu um esforço considerável para contextualizá-la enquanto problema de gestão pública, focando na actuação institucional e nos mecanismos administrativos de prevenção e resposta a incidentes cibernéticos. A segunda limitação foi a demora no agendamento da entrevista com o INTIC, que levou cerca de quatro meses, comprometendo o cronograma da pesquisa. Por fim, o entrevistado não respondeu a todas as perguntas formuladas, o que limitou a profundidade da análise empírica.

CAPÍTULO IV: APRESENTAÇÃO, ANÁLISE, DISCUSSÃO E INTERPRETAÇÃO DE DADOS

4. Apresentação e caracterização do INTIC[2]

O INTIC é o órgão responsável por regular, supervisionar e fiscalizar o sector das Tecnologias de Informação e Comunicação (TIC) no nosso país. Sua génese foi a Unidade Técnica de Implementação da Política de Informática (UTIC), criada em 2002 para assessorar o Governo na introdução de TIC, tendo este estatuto vigorado até 2014, quando foi transformado no actual figurino de instituto público.

Inicialmente, tratou-se de um órgão bicéfalo, exercendo funções implementadoras e regulatórias ao mesmo tempo. Mas a Lei no 3/2017, de 9 de Janeiro, que estabelece os princípios, as normas gerais e o regime jurídico das transacções electrónicas em geral, do comércio electrónico e do governo electrónico em particular, acabaria com o regime bicéfalo ao designar o INTIC como a Entidade Reguladora da referida lei e remeter ao executivo a tarefa de criar uma autoridade de governo electrónico, que é o Instituto Nacional do Governo Electrónico (INAGE).

Assim, o INTIC passou a ocupar-se, entre outras funções, exclusivamente de:

- Garantir um ambiente seguro para Sociedade de Informação;
- Registar e licenciar provedores de serviços de TIC;
- Estabelecer regras de funcionamento do sector das TIC;
- Fiscalizar o cumprimento da legislação e outras normas do sector das TIC;
- Aplicar as penalizações;
- Promover políticas e boas práticas para o uso das TIC.

Como corolário da implementação da referida lei, a organização e funcionamento do INTIC foram revistos pelo Decreto no 90/2020, de 9 de Outubro, que materializa a vontade estatal de um maior controlo sobre a Sociedade de Informação, pela via da administração indirecta, em conformidade com o novo regime jurídico dos institutos, fundações e fundos públicos, aprovado pelo Decreto no 41/2018, de 23 de Julho.

[2] https://intic.gov.mz/apresentacao/

Estrutura orgânica

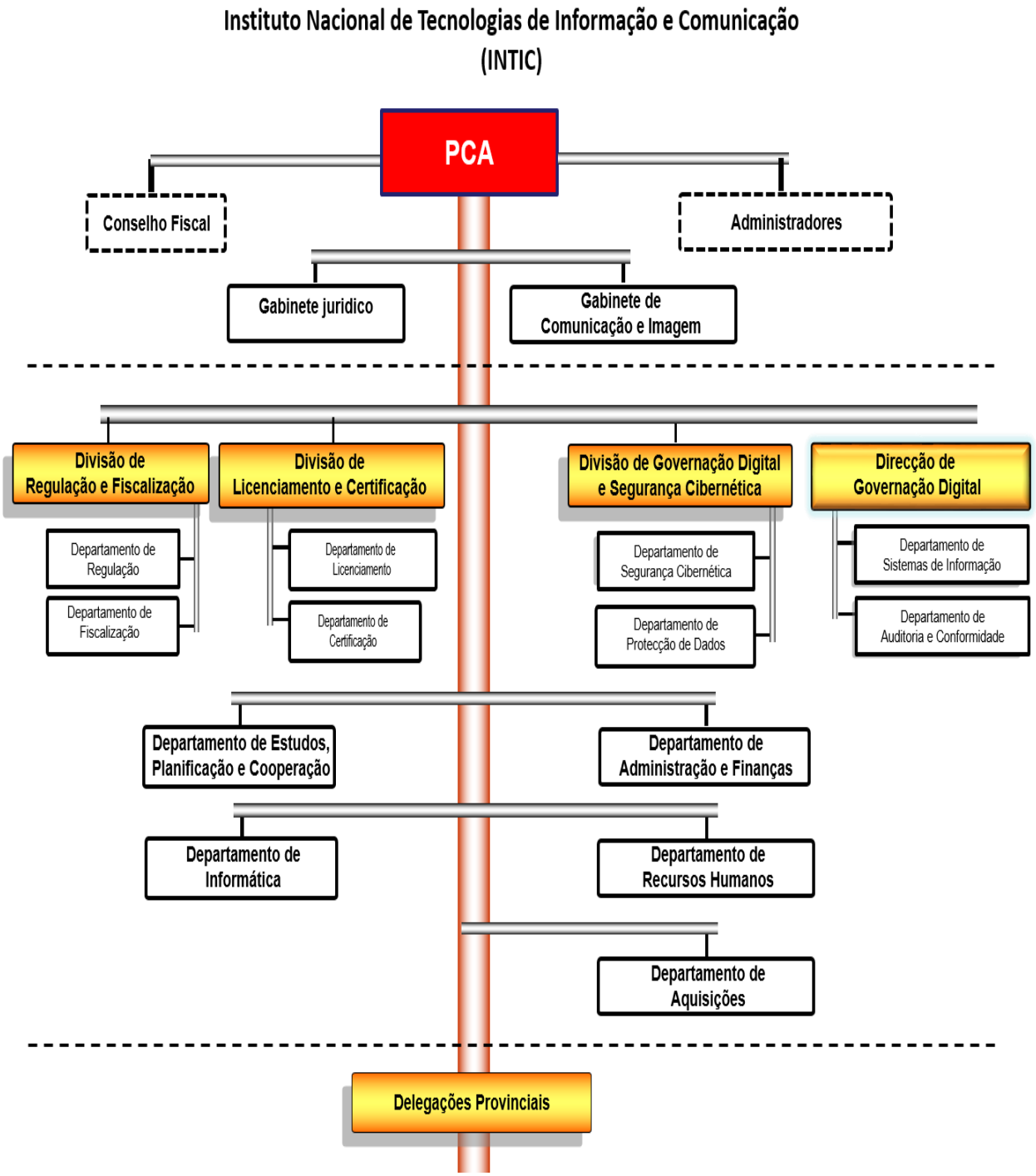


Figura 04: estrutura orgânica do INTIC (MASSUNGUINE, 2022, 37)

4.1. Os ataques cibernéticos mais recorrentes no e-GOV em Moçambique

Nos últimos anos, Moçambique tem enfrentado um aumento expressivo na incidência de ataques cibernéticos no e-GOV, reflectindo uma tendência global de crescimento e evolução das ameaças digitais. Segundo o Relatório de Segurança Cibernética na África de 2023, as principais formas de ataques envolvem *phishing*, *ransomware*, *malware* e tentativas de acesso não autorizado a redes governamentais, financeiras e empresariais (ACRSS, 2023). Esses incidentes têm causado impactos severos na infra-estrutura crítica do país, prejudicando sectores essenciais como energia, telecomunicações, saúde e bancos, além de comprometerem informações sensíveis de cidadãos e instituições.

A expansão do uso de tecnologias digitais, principalmente impulsionada pela pandemia de COVID-19, acelerou a disseminação destes ataques (INE, 2022). Para o entrevistado E1, os maiores vectores de ameaça percebidos são o phishing, DDoS e invasões as pessoas com informações privilegiadas. Segundo suas palavras:

> No e-GOV, os ataques mais recorrentes costumam ser os que exploram falhas básicas de segurança, como *phishing*, onde o golpista tenta enganar servidores públicos ou cidadãos para roubar dados sensíveis; ataques de negação de serviço (DDoS), que sobrecarregam os sistemas e tiram os serviços do ar; e invasões que exploram vulnerabilidades em sistemas desactualizados ou mal configurados, também têm muita preocupação com vazamento de dados, especialmente porque os sistemas de governo lidam com informações pessoais de milhões de pessoas. (E1)

Portanto, Botacin e Grégio (2021), argumentam que muitos sistemas de governo electrónico ainda possuem vulnerabilidades técnicas e de configuração que os tornam alvos frequentes de ataques, além de apresentarem baixa maturidade em práticas de segurança. Essas vulnerabilidades decorrem, em grande parte, da adopção de infra-estruturas tecnológicas desactualizadas e da ausência de processos padronizados de segurança. Em muitos casos, as instituições públicas utilizam sistemas desenvolvidos há vários anos, que não acompanham as exigências atuais de protecção digital.

Ataques de *phishing* exploram a vulnerabilidade humana por meio de técnicas de engenharia social, com o objectivo de enganar usuários e obter acesso a dados sensíveis, e, ataques do tipo *DDoS* continuam sendo utilizados por sua capacidade de derrubar serviços públicos digitais, muitas vezes hospedados em infra-estruturas centralizadas e pouco resilientes, o que causa

prejuízos e instabilidade na prestação de serviços à população (Ahmed et al., 2022, Guzella Dias et al., 2024).

Apesar do crescimento na adopção de soluções de segurança, Moçambique ainda apresenta lacunas na formação de profissionais especializados em cibersegurança, dificultando a implementação de acções de defesa eficazes (ITU, 2022). Além disso, muitos sectores estratégicos de digitalização de serviços públicos e privados, ampliando a superfície de ataque dos cibercriminosos continuam vulneráveis a ataques, como resultado, cresce a ameaça de roubos de dados, extorsões e paralisações de serviços essenciais, o que pode afectar directamente a estabilidade económica e social do país (Idem).

No que concerne à autoria dos ataques cibernéticos contra as plataformas de e-GOV, verificou-se, a partir das informações fornecidas pelo entrevistado E1, que:

> os ataques cibernéticos ao e-GOV geralmente são realizados por diferentes tipos de agentes, incluindo cibercriminosos que procuram ganhar dinheiro; grupos organizados (como caso de piratas informáticos e terroristas) com capacidade técnica para explorar falhas nos sistemas, pessoas internas com acesso privilegiado que podem agir por motivos pessoais, e em alguns casos, até grupos ligados a governos estrangeiros com interesses políticos. (E1)

O que está em consonância com a Avaliação Nacional de Riscos Cibernéticos (NCRA, 2025), segundo a qual, no país, os maiores atores de ameaças cibernéticas são os piratas informáticos amadores, seguidos pelos cibercriminosos e pelos terroristas cibernéticos, que representam preocupações igualmente significativas. Em outros sectores, como Finanças, os piratas informáticos amadores representam o principal problema, enquanto sectores como energia também se preocupa muito com terroristas cibernéticos.

Olhando para os sectores mais impactados dentro do e-GOV, destaca-se o sector da segurança pública, cujos sistemas informáticos se mostram especialmente vulneráveis a ataques provenientes de agentes estatais, terroristas cibernéticos, cibercriminosos e activistas políticos digitais. Esses agentes podem utilizar diversos vectores de ameaça, como *softwares* maliciosos, *phishing* (fraude electrónica), comprometimento da cadeia de abastecimento ou mesmo acções de pessoas com acesso privilegiado aos sistemas. Todos esses vectores são classificados como de alta ameaça no contexto da segurança digital governamental (NCRA, 2025, 16).

4.2. Factores que tornam o e-GOV de Moçambique vulnerável a ataques cibernéticos

Conforme referido, Moçambique tem enfrentado diversos incidentes cibernéticos nos últimos anos, o que evidencia fragilidades significativas na segurança digital das instituições públicas. Um dos casos mais emblemáticos ocorreu em Fevereiro de 2022, quando vários portais governamentais, como os do Instituto Nacional de Gestão de Desastres (INGD), Administração Nacional de Estradas (ANE), Administração Regional de Águas do Sul e Instituto Nacional de Transportes Terrestres (INATTER), foram temporariamente desactivados após sofrerem ataques cibernéticos. As páginas foram substituídas por mensagens de autoria dos invasores, o que demonstrou não apenas vulnerabilidades técnicas, mas também impactos directos na confiança institucional, na continuidade dos serviços públicos e na privacidade dos dados dos cidadãos (TEMBE, 2024).

Esse episódio evidenciou como a interdependência e interoperabilidade dos sistemas, características centrais do governo electrónico, introduzem novas camadas de risco e aumentam a superfície de ataque. Diferentemente da burocracia tradicional mais isolada e fragmentada, o e-GOV funciona com redes integradas, que, quando mal protegidas, tornam-se susceptíveis a ameaças externas e ataques coordenados.

Para o entrevistado E1, um dos factores que tornam o e-GOV vulnerável aos ataques cibernéticos em Moçambique é o uso de TIC que ainda não atingiram um nível de desenvolvimento suficiente para enfrentar de forma eficaz tais ameaças. Em suas palavras, esclareceu que:

> Primeiramente, diversos sistemas governamentais continuam a operar com tecnologias obsoletas, que já não recebem actualizações regulares de segurança. Essa desactualização compromete significativamente a integridade dos sistemas, criando vulnerabilidades que podem ser facilmente exploradas por agentes maliciosos [...].

Segundo Madan (2024), os chamados *legacy systems* (sistemas legados) muitas vezes ineficientes e ultrapassados, representam um obstáculo à modernização dos serviços públicos e são particularmente vulneráveis a ameaças cibernéticas, uma vez que não oferecem suporte adequado a padrões modernos de segurança. Essa limitação tecnológica compromete a capacidade de resposta dos sistemas frente aos novos tipos de ataques digitais.

De forma semelhante, Govindaraaj (2023) argumenta que as restrições inerentes a esses sistemas, como a ausência de actualizações regulares, o não uso de protocolos de segurança e a incompatibilidade com técnicas modernas de encriptação, criam um ambiente propício à exploração por agentes maliciosos. No contexto da Administração Pública, tais limitações tornam-se ainda mais críticas, uma vez que os sistemas governamentais sustentam serviços essenciais à população e armazenam grandes volumes de dados sensíveis.

Akinsanya (2025)**,** por sua vez, enfatiza que muitos desses sistemas antigos continuam a ser a espinha dorsal das instituições públicas, mas acabam se tornando "pontos cegos" no que diz respeito à segurança cibernética, pois são essenciais demais para serem substituídos de imediato**,** mas vulneráveis demais para permanecerem sem adaptações**.**

Além disso, segundo o entrevistado E1, existe uma carência de políticas padronizadas de cibersegurança entre os diferentes órgãos do Estado. Em muitos casos, práticas básicas de protecção da informação, como a utilização de senhas fortes e políticas de autenticação seguras, não são aplicadas de forma uniforme nas instituições públicas. Essa realidade, conforme observa o entrevistado, evidencia a ausência de uma cultura organizacional orientada para a segurança da informação. Outro factor considerado crítico é a escassez de profissionais qualificados em cibersegurança no sector público. O E1 enfatiza que a falta de técnicos especializados compromete a implementação efectiva das medidas de protecção, bem como o monitoramento contínuo dos sistemas e a resposta rápida a incidentes que afectam o e-GOV. A falta de capacidade técnica compromete a implementação de medidas preventivas, dificulta o monitoramento contínuo dos sistemas e reduz a eficácia das respostas em caso de incidentes. A situação é agravada ainda pela limitada formação dos funcionários públicos em práticas seguras de uso digital. Muitos servidores não reconhecem os riscos de acções simples como clicar em *links* suspeitos ou utilizar dispositivos pessoais em redes institucionais, tornando-se alvos fáceis de ataques como *phishing* e engenharia social.

Como destaca Kizza (2020), as vulnerabilidades cibernéticas estão directamente relacionadas não apenas à tecnologia utilizada, mas também à governança deficiente dos activos digitais, dos sistemas e das pessoas que os operam.

Marcelino (2014) reforça que a obsolescência tecnológica, a ausência de regras claras de gestão de riscos, e a escassez de pessoal capacitado são obstáculos significativos para o amadurecimento da segurança cibernética em países em desenvolvimento.

Embora o país tenha dado passos importantes como a criação do Centro Nacional de Resposta a Incidentes Cibernéticos (CERT-MZ), em 2015, subordinado ao Ministério da Ciência, Tecnologia e Ensino Superior e Técnico-Profissional (MCTESTP), os avanços ainda são limitados. Em Setembro de 2020, por exemplo, a equipa do CERT-MZ era composta por apenas seis especialistas (MOÇAMBIQUE, 2020b), o que evidencia a fragilidade institucional para enfrentar ameaças de grande escala.

Portanto, a combinação entre infra-estrutura tecnológica deficiente, ausência de políticas integradas de cibersegurança, falta de capacitação técnica e pouca sensibilização dos servidores públicos forma um cenário de alta vulnerabilidade. Em um contexto de crescente digitalização dos serviços estatais, tais fragilidades representam riscos concretos para a estabilidade, a soberania digital e a confiança da população no e-GOV moçambicano.

4.3. O papel desempenhado pelo INTIC no combate e prevenção dos ataques cibernéticos no e-GOV

Nos últimos anos, o INTIC tem desempenhado um papel fundamental no fortalecimento da infra-estrutura digital de Moçambique e na implementação de estratégias de segurança cibernética. Como órgão responsável pelo desenvolvimento e regulação das TIC no país, o INTIC tem promovido acções para estimular a inovação, ampliar o acesso às tecnologias digitais e aprimorar as capacidades de protecção dos sistemas nacionais contra ameaças cibernéticas (INTIC, 2023). No caso concreto dos ataques cibernéticos, nas suas principais iniciativas, destacam-se a elaboração de políticas de governança digital, a criação de Centros de Resposta a Incidentes de Segurança Computacional (CSIRC) e a disseminação de boas práticas de segurança entre órgãos públicos e empresas privadas (INTIC, 2023).

Além disso, o INTIC tem liderado programas de capacitação destinados a formar profissionais especializados em cibersegurança, reconhecendo a necessidade de formar uma força de trabalho qualificada para responder às crescentes ameaças digitais (INTIC, 2022).

No que diz respeito às acções que têm sido implementadas por essa instituição no âmbito da segurança cibernética do e-GOV, o E2 referiu-que "a cibersegurança do Estado está sendo fortalecido através de normas claras, capacitação dos técnicos, monitoria constante dos sistemas e cooperação com parceiros, para garantir uma resposta mais rápida e eficaz aos ataques".

Outro especto importante é a implementação de campanhas de sensibilização voltadas para a sociedade civil, empresários e instituições públicas, na tentativa de reduzir vulnerabilidades causadas pelo uso inadequado da tecnologia, especialmente nas áreas de protecção de dados pessoais e privacidade. Nesse sentido, o INTIC também tem colaborado com outros órgãos do governo e organizações internacionais na elaboração de marcos regulatórios e legislações relacionadas à segurança da informação, contribuindo para um ambiente digital mais seguro e confiável (INTIC, 2023).

O instituto vem actuando na digitalização de serviços públicos, o que aumenta a eficiência governamental, mas também exige a criação de mecanismos robustos de defesa contra ataques cibernéticos. Para isso, o INTIC tem buscado implementar soluções tecnológicas avançadas e estabelecer parcerias internacionais, com o objectivo de promover a troca de informações sobre ameaças emergentes e adoptar as melhores práticas globais de cibersegurança (INTIC, 2022). Estas acções apontam para a melhoria da nossa cibersegurança nos últimos anos, conforme mostra o gráfico abaixo.

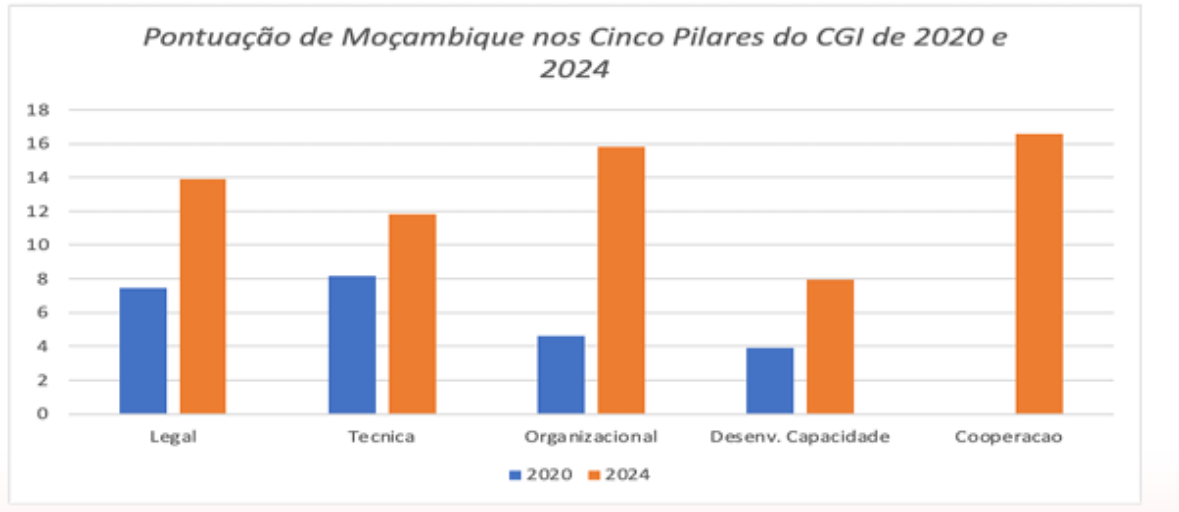


Gráfico 02: Gráfico Comparativo da Evolução de Moçambique no Índice Global de Cibersegurança (INTIC, 2024)

Moçambique tem registado avanços significativos no domínio da cibersegurança, posicionando-se actualmente como o país mais bem classificado entre os PALOP (Países Africanos de Língua Oficial Portuguesa) no Índice Global de Segurança Cibernética (GCI), elaborado pela União Internacional das Telecomunicações (UIT). Segundo dados da edição de 2024 do GCI, Moçambique passou de cerca de 24,19 pontos em 2020 para aproximadamente 66,05 pontos, um crescimento de mais de 41 pontos (INTIC, 2024). Este desempenho destaca o país não apenas no contexto dos PALOP, mas também como um dos que mais evoluiu em África no sector da cibersegurança. O progresso moçambicano resulta de um conjunto de acções estratégicas, com destaque para os avanços nos pilares organizacional e de cooperação, que foram os que mais contribuíram para o salto na classificação (INTIC, 2024).

O país tem apostado no fortalecimento das instituições que lidam com a segurança digital, como o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), e na criação de estruturas para resposta a incidentes, além de promover maior articulação entre os sectores público, privado e académico.

Como explica Silva (2021), a eficiência do INTIC reside na implementação de estratégias de monitoramento contínuo, análise de vulnerabilidades e desenvolvimento de soluções de segurança adaptadas às ameaças emergentes, Oliveira (2020) acrescenta a capacidade do INTIC de integrar tecnologias avançadas, como inteligência artificial e análise comportamental, aumenta sua precisão na detecção precoce de invasões, permitindo respostas rápidas que minimizam danos e prejuízos ao sistema público. Relativamente ao desempenho e à eficiência deste instituto, o entrevistado destacou que

> a eficiência do INTIC na detecção de ataques cibernéticos ao e-GOV tem vindo a dar passos positivos nos últimos anos. Um dos pontos fortes é o esforço contínuo na criação de políticas e normas que orientam as instituições públicas sobre como proteger os seus sistemas. O INTIC também tem investido em capacitação técnica, promovendo formações em cibersegurança para técnicos do sector público, o que tem ajudado a melhorar a capacidade de identificar ameaças mais rapidamente. (E2)

Creese (2014) defende que, para garantir protecção eficaz, inclusive no sector público, é vital investir em modos robustos de detecção, em estruturas organizacionais resilientes e em

capacidades técnicas que identifiquem ameaças proactivamente. O INTIC tem-se mostrado eficiência no combate aos ataques cibernéticos ao e-GOV ao implementar medidas robustas de segurança, como *firewalls*, sistemas de detecção de intrusão e protocolos de resposta rápida. Sua actuação contribui para a diminuição de vulnerabilidades e aumenta a resiliência da infra-estrutura digital governamental, garantindo maior protecção dos dados dos cidadãos e a continuidade dos serviços públicos electrónicos.

A eficácia do INTIC, por sua vez, é reflectida nos resultados concretos de seus programas de treinamento e capacitação de servidores públicos, que melhoraram significativamente a postura de segurança do governo. Estudos indicam que a realização de simulados e treinamentos periódicos contribui para uma maior sensibilização e preparação das equipes, fortalecendo a resiliência institucional frente a ataques (PEREIRA & SOUZA, 2019).

Ademais, a criação de normativas específicas, alinhadas às melhores práticas internacionais, reforça o quadro regulatório e promove uma cultura de segurança mais sólida entre os órgãos governamentais. Ademais, o INTIC atua na coordenação com entidades internacionais, ampliando a capacidade de resposta e compartilhamento de informações sobre ameaças cibernéticas, o que promove uma actuação colaborativa mais eficiente (INTIC, 2022).

A integração de bases de dados e o intercâmbio de inteligência possibilitam uma abordagem mais proactiva na prevenção de ataques, transcorrendo de uma actuação reactiva para uma estratégia de defesa preditiva (COSTA, 2023).

Para Lima (2021)., desafios persistem, como a necessidade de investimentos constantes em tecnologias de ponta e na formação de profissionais especializados, aspectos apontados como essenciais para manter elevados níveis de eficiência e eficácia

Relacionado a questão da eficácia, O entrevistado E1 comentou, de modo geral, que o INTIC tem conseguido reduzir significativamente os riscos cibernéticos, aumentando a capacidade de defesa dos sistemas. Segundo ele, a instituição tem se tornado mais eficaz não apenas na prevenção de ataques, mas também na resposta rápida a qualquer ameaça (E2). Assim, O INTIC demonstra alta eficácia na implementação de estratégias de defesa cibernética, utilizando tecnologias avançadas e monitoramento contínuo para detectar e neutralizar ameaças em tempo real. Sua eficácia é evidenciada pela redução de incidentes de segurança e pelo fortalecimento

das defesas das instituições sob sua gestão, promovendo um ambiente digital mais seguro e confiável.

Quanto a questão referente responsabilização, de 2020 à 2023, o INTIC desempenhou papel central na criação, operacionalização e responsabilização institucional no combate a ataques cibernéticos através da estrutura nacional de resposta a incidentes (nCSIRT), conforme a Política e Estratégia Nacional de Segurança Cibernética (Resolução 69/2021).

Em Setembro de 2023, o INTIC anunciou que Moçambique enfrentava em média 1,5 milhões de ataques cibernéticos por mês**,** destacando a gravidade da situação e a prevalência de fraudes electrónicas, burlas, roubo de dados e ataques a infra-estruturas críticas, reforçando a necessidade de atenção estratégica imediata. Para mitigar riscos, o INTIC realizou entre Setembro de 2023 e Abril de 2024 a primeira avaliação nacional de riscos cibernéticos em infra-estruturas críticas, com vista a mapear vulnerabilidades estratégicas em sectores sensíveis e estados institucionais vulneráveis.[3] O Workshop realizado em Julho de 2024, em cooperação com o Programa Global de Crimes Cibernéticos da ONUDC, permitiu a apresentação do relatório de avaliação de capacidades nacionais, identificando os principais tipos de crimes cibernéticos e lançando as bases para o Plano de Acção legislativo e operacional em curso pelo INTIC. Por outro lado, o PCA do INTIC declarou em 2024 que, embora não seja possível eliminar completamente os ataques, esperava mitigá-los através da proactividade, educação pública e resposta activa evidenciando compromisso institucional à responsabilidade operacional contínua, ainda que reconhecendo limitações estruturais.[4]

4.4. As principais consequências dos ataques cibernéticos no e-GOV

Com o avanço da digitalização em Moçambique, os sistemas de informação tornaram-se cada vez mais essenciais para o funcionamento das instituições públicas e privadas. No entanto, essa dependência tecnológica também tem exposto o país a uma crescente onda de ameaças cibernéticas. Segundo o INTIC (2023), os ataques cibernéticos têm causado impactos significativos em diversas áreas, comprometendo a segurança, a privacidade e a estabilidade das infra-estruturas digitais. Os impactos não se limitam apenas ao dinheiro, mas também aos

[3] https://intic.gov.mz/intic-realiza-primeiro-workshop-de-avaliacao-de-riscos-de-seguranca-cibernetica/
[4] https://www.diarioeconomico.co.mz/2023/02/15/trends/tech/intic-nao-vamos-acabar-com-ataques-ciberneticos-mas-esperamos-mitiga-los/

serviços críticos afectados por ataques cibernéticos. Embora os sectores de Energia, finanças e transporte fossem severamente afectados, os impactos dos ataques cibernéticos em Moçambique afectariam muitos outros sectores, com o de Tecnologia de Informação e comunicação, sofrendo impactos significativos (NCRA:2025:11).

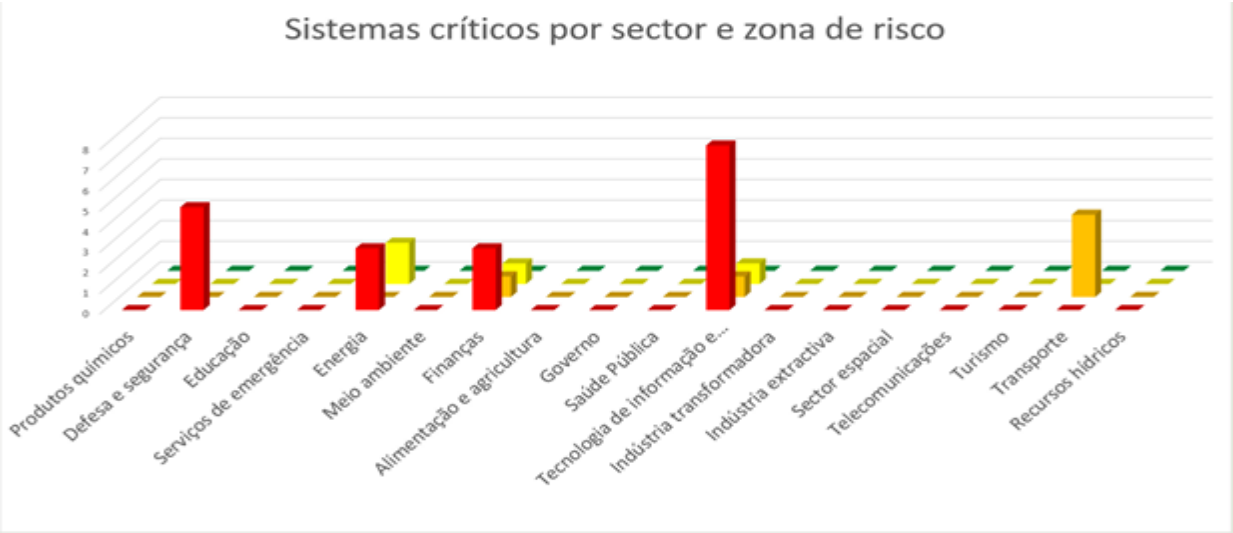


Gráfico 03: Impacto do risco cibernético em sectores críticos (NCRA, 2025, 11)

Os dados mostram que o impacto dos riscos cibernéticos nos serviços públicos em Moçambique é significativo, especialmente nos sectores da defesa e segurança, em que podem comprometer a segurança nacional, permitindo que informações confidenciais sejam acessadas por atores mal-intencionados; No sector da energia, a vulnerabilidade aos ataques cibernéticos pode levar a interrupções no fornecimento de energia e afectar a economia e a segurança; e no sector de tecnologia de comunicação e informação, onde os serviços públicos dependem cada vez mais da tecnologia para fornecer aos cidadãos, tornando-os vulneráveis a ataques cibernéticos. A perda de dados ou a interrupção dos serviços de TIC pode afectar a confiança dos cidadãos nos serviços públicos e comprometer a governação eficaz (NCRA, 2025, 12).

No que diz respeito as consequência, conforme avança a fonte ouvida, os ataques cibernéticos têm causado consequências bastante sérias no país, referindo que:

> Um dos impactos mais imediatos é a interrupção de serviços essenciais, como os sistemas bancários, plataformas governamentais ou de saúde, o que afecta directamente o dia-a-dia dos cidadãos. Também temos registado a perda ou o vazamento de dados sensíveis, tanto pessoais quanto institucionais, o que levanta preocupações com a privacidade e a protecção

> de informação. Além disso, os prejuízos financeiros são significativos, pois as instituições gastam muito na recuperação dos sistemas e na resposta a incidentes. Outro ponto importante é o dano à reputação das organizações afectadas quando há falhas de segurança, a confiança do público tende a diminuir. (E1)

O que está em consonância com Sedenberg e Dempsey (2018), que alertam para o impacto desses ataques sobre dados sensíveis do governo e a necessidade urgente de estruturas eficazes de governança e compartilhamento de informações no sector público.

Diante das consequências identificadas pelo INTIC, que vão desde a interrupção de serviços essenciais até a exposição de dados sensíveis e prejuízos económicos significativos, torna-se evidente a necessidade urgente de um investimento contínuo em infra-estruturas de segurança digital, capacitação técnica e desenvolvimento de políticas eficazes de prevenção e resposta a incidentes, com o objectivo de mitigar os impactos dos ataques cibernéticos e assegurar a integridade, disponibilidade e confidencialidade dos sistemas informáticos a nível nacional.

4.5. Desafios do INTIC no combate aos ataques cibernéticos

O INTIC enfrenta desafios significativos no combate aos ataques cibernéticos, especialmente relacionados às limitações tecnológicas, estruturais e à escassez de recursos humanos, que comprometem a segurança digital governamental.

Um dos grandes obstáculos ao combate eficaz aos ciberataques no ambiente e-GOV é a falta de coordenação entre entidades públicas. O Ministério das Comunicações e Transformação Digital (MCTD), o INTIC, a SERNIC, Procuradoria, órgãos sectoriais e municipalidades ainda operam com estruturas desarticuladas, o que prejudica a criação de uma estratégia unificada de defesa cibernética. Além disso, a actuação descentralizada compromete a implementação uniforme de protocolos de segurança em serviços e-GOV distribuídos, o que abre brechas que exploradores cibernéticos tendem a identificar e explorar (INTIC, 2023). Para aquele profissional,

> A inexistência de um sistema de informação que possa hospedar os diferentes sistemas das instituições públicas dificulta no combate aos ataques cibernéticos, pois, para cada um destes, exigirão tratamentos diferenciados, o que por sua vez, impossibilita a adopção de uma e única estratégia para todo o sistema do e-GOV. E2

Como destacam Jang e Lim (2013), a falta de alinhamento entre os órgãos de segurança cibernética e de aplicação da lei compromete a eficácia das respostas institucionais, exigindo estruturas de cooperação mais robustas. Com isso, o país estará mais preparado e protegido no ambiente digital.

Embora o Estado tenha aprovado normas para identificação de infra-estruturas críticas de informação, a implementação física ainda é lenta e desigual entre ministérios e outras instituições públicas. Muitos organismos públicos dependem de servidores desactualizados e certificação digital incompleta, o que reduz a sua capacidade de resistir a ataques sofisticados. A falta de *frameworks* de interoperabilidade seguros entre plataformas de governo digital agrava o risco de propagação de incidentes cibernéticos entre serviços conectados (PNUD, 2025). A adopção de ferramentas energizadas em nuvem é ainda incipiente e pouco regulamentada, o que impacta a segurança e soberania dos dados governamentais. Nisto, o nosso E2 argumentou que

> No combate aos ataques cibernéticos, as limitações tecnológicas e de infra-estrutura no e-GOV são um desafio constante. Sistemas antigos e a falta de integração entre plataformas dificultam respostas rápidas e eficientes. Também precisamos avançar no uso seguro da nuvem para proteger melhor os dados governamentais (…) E2.

Para o entrevistado E1, as limitações na base tecnológica e nas infra-estruturas que sustentam o governo electrónico (e-GOV) podem representar um desafio adicional no combate aos ataques cibernéticos. Em alguns contextos, nota-se a existência de sistemas desactualizados, falta de interoperabilidade e carência de recursos técnicos que podem afectar a eficácia das respostas a incidentes. Por isso, o reforço da infra-estrutura digital e a modernização contínua dos sistemas são vistos como medidas importantes para fortalecer a segurança e a confiança nos serviços públicos digitais.

Outro desafio significativo enfrentado pelo INTIC diz respeito à escassez de profissionais qualificados na área de cibersegurança dentro das instituições públicas. Apesar dos avanços normativos e da crescente digitalização dos serviços estatais, o ritmo de formação e capacitação de técnicos especializados não tem acompanhado a sofisticação crescente das ameaças cibernéticas. Como resultado, muitas instituições públicas operam com equipas reduzidas ou sem qualquer especialista dedicado à segurança digital, o que compromete tanto a prevenção quanto a

resposta eficaz a incidentes (ITU, 2021). Além disso, a alta competitividade do sector privado na área de tecnologia da informação torna difícil para o sector público atrair e reter profissionais com competências técnicas avançadas.

A ausência de incentivos salariais, planos de carreira atractivos e programas regulares de actualização profissional agrava esse cenário. Como destaca o Programa das Nações Unidas para o Desenvolvimento (PNUD, 2025), a resiliência digital dos governos depende não apenas de investimentos em infra-estrutura, mas também da qualificação contínua dos seus recursos humanos. Nesse sentido, o fortalecimento do capital humano especializado deve ser considerado uma prioridade estratégica na consolidação da cibersegurança do e-GOV moçambicano, cabendo ao INTIC e a outras entidades públicas investir em programas de formação, certificação e retenção de talentos no sector.

CAPITULO V: CONCLUSÃO E RECOMENDAÇÕES

Conclusão

Este trabalho teve como propósito analisar às ameaças digitais enfrentadas no e-GOV entre os anos 2020-2023, olhando para o desempenho do INTIC. A pesquisa permitiu identificar os principais desafios enfrentados pela instituição, bem como os avanços alcançados na promoção da cibersegurança no sector público. No país, os ataques ao e-GOV destacam-se o *phishing*, negação de serviço (DDoS), *ranswore*, e a proliferação de *malwares*, isto tem demonstrado o quanto os sistemas do sector público ainda são frágeis diante das ameaças cada vez mais complexas e sofisticadas. Essas ameaças podem ter motivações políticas, económicas ou ideológicas, afectando não apenas a confiança da população nos serviços públicos, mas também a estabilidade e soberania digital do país.

Entre os factores que fragilizam os sistemas de governo electrónico em Moçambique, destacam-se a carência de profissionais qualificados em segurança digital e o uso de tecnologias ultrapassadas, muitas vezes mal implementadas. Esses problemas comprometem significativamente a capacidade de resposta das instituições públicas diante de incidentes cibernéticos e aumentam os riscos de falhas nos serviços. Diante desse cenário, torna-se evidente a necessidade de investimentos contínuos em formação técnica, modernização dos sistemas e criação de uma cultura institucional voltada para a segurança digital em todos os níveis da administração pública. Neste cenário, o papel do INTIC é de extrema relevância.

Como órgão responsável por coordenar as políticas de tecnologias de informação e comunicação no sector público, o INTIC tem se empenhado em promover acções de sensibilização, formação e regulamentação do uso seguro das tecnologias digitais. A instituição tem colaborado activamente na construção de instrumentos legais e normativos voltados para a actuação no ciberespaço moçambicano, buscando estabelecer directrizes claras e mecanismos de protecção adequados às especificidades do contexto nacional. Ainda assim, os esforços do INTIC são limitados pela falta de recursos financeiros, tecnológicos e humanos, o que restringe a sua capacidade de resposta e intervenção em larga escala. É importante destacar que a eficácia das políticas de cibersegurança depende não apenas da actuação isolada do INTIC, mas de uma acção coordenada entre diferentes instituições do Estado, do sector privado, da academia e da sociedade civil.

Recomendações

- Actualização e implementação efectiva da Estratégia Nacional de Cibersegurança,
- Criação de um quadro regulatório robusto para segurança da informação em órgãos públicos.
- Estabelecimento de políticas claras de segurança para o sector público digital.
- Treinamento contínuo de funcionários públicos em práticas de cibersegurança (phishing, gestão de senhas, uso seguro da internet).
- Campanha de educação digital para o cidadão, aumentando a literacia em cibersegurança.
- Criação de programas de formação técnica avançada para profissional TIC do sector público.
- Garantir que todos os sistemas do e-GOV estejam em conformidade com a Lei de Protecção de Dados Pessoais.
- Criptografia de dados sensíveis em trânsito e em repouso.

Referências bibliográficas

- AKINSANYA, Ayo. *My top five security considerations in legacy system modernization*. ISC², 2025.
- ALMEIDA, Ítalo D'Artagnan. *Metodologia do Trabalho Científico*. Recife: UFPE, 2021.
- ASLLANI, Mejreme. *Cyber-attacks and critical infrastructure in Kosovo*. Young Faces DCAF 2022 Participant. [S.l.]: DCAF, 2022.
- BÄCHTOLD, Ciro. *Noções de Administração Pública*. Curitiba PR: [s.n.], 2012.
- BARROS, Martina Jennifer Zucule; NIEKERK, Brett Van. *Cybersecurity in Mozambique: status and challenges*. In: Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS, Vol. 22, No. 1. [S.l.]: ECCWS, 2023.
- BELLO, J. L. P. *Metodologia Científica: manual para elaboração de monografias*. Rio de Janeiro: UVA, 2009.
- BRASIL. Gabinete de Segurança Institucional da Presidência da República. *Cartilha de Segurança para Internet*. CERT.br/NIC.br, 2021.
- BUCKLAND, Benjamin S.; SCHREIER, Fred; WINKLER, Theodor H. *Democratic governance challenges of cyber security*. Horizon, 2015. [S.l.]: Horizon, 2015.
- CEPIK, Marco Aurélio Chaves; MARCELINO, Henriques Manuel. *Segurança cibernética em Moçambique: conceitos, infra-estrutura, desafios de implementação*, 2022.
- DENCKER, Ada de Freitas Maneti. *Métodos e técnicas de pesquisa em turismo*. 4. ed. São Paulo: Futura, 2000.
- ECLAIR, Jane L. "*Cybersecurity workforce challenges in government agencies: Addressing skill gaps and retention*." Government Information Quarterly, v. 34, n. 4, p. 101–110, 2017.
- FERNANDO, Júlio. *Os Desafios e Resultados das Formações nos Centros Provinciais de Recursos Digitais (CPRD) no âmbito do Govnet em Moçambique: O caso do INTIC/CPRD Nampula*, 2016.
- FERREIRA, Carlos. *Cibersegurança e governo electrónico em África: desafios e oportunidades*. Maputo: Centro de Estudos de Governança, 2021.
- GIL, A. C. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2008.
- GOVINDARAAJ, Surya. *Analyzing the effectiveness of data security policies in legacy systems*. Research Gate, 2023.

- HIRSCH, Paulo Josef. *Construindo o governo do séc. XXI: uma arquitectura organizacional orientada para o cidadão*. [s.l.]: [s.n.], 2003.
- INTIC; *Relatório sobre o Estado da Cibersegurança em Moçambique,* 2020-2023
- JANG, Yunsik Jake; LIM, Bo Young. "*Cybersecurity Policy and Coordination in Korea: Harmonizing Government Agencies for National Cybersecurity*." 2013.
- JOÃO, Atália Ana Maria. *Análise do impacto do Sistema de Gestão Documental na prestação de Serviços Públicos na Direcção do Registo Académico da Universidade Eduardo Mondlane: uma Reflexão a partir do serviço de emissão do Certificado de Habilitações Literárias – (2020-2022)*, 2023.
- JUNIOR, António Bai Sitoe. *Governos electrónicos em Moçambique e os dilemas de accountability vertical no contexto da COVID 19*, 2022.
- KAUARK, F. S. et al. *Metodologia da Pesquisa: Um guia prático*. Itabuna/Bahia: Via Litterarum, 2010.
- KIZZA, Joseph Migga. *Guide to Computer Network Security*. 5. ed. Cham: Springer, 2020.
- LAKATOS, E. M.; MARCONI, M. de A. *Fundamentos de metodologia científica*. 6. ed., São Paulo: Atlas, 2007.
- MADAN, Mona. *Challenges and strategies in modernizing legacy systems in public administration*. Walsh Medical Media, 2024.
- MADZOVA, Vesna; BIANCHI, Carmine; DI BITETTI, Mario. *The impact of legacy systems on digital transformation in European public administration: lessons learned from a multi-case analysis*. Government Information Quarterly, [S.l.], 2022.
- MAY, T. *Pesquisa social: questões, métodos e processos*. 3. ed. Porto Alegre: Artmed, 2004.
- Mozambique Data Diagnostic; INAGE-INTIC 2025
- MULLER, Lilly Pijnenburg. *Cyber security capacity building in developing countries: challenges and opportunities*. [s.l.], [s.d.].
- PRODANOV, C. C.; FREITAS, E. C. *Metodologia do Trabalho Científico: métodos e técnica da pesquisa e do trabalho académico*. 2. ed. Novo Hamburgo: Feevale, 2013.

- PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (PNUD). "*Fraca infra-estrutura e baixa conectividade ainda são obstáculos à digitalização em Moçambique – PNUD*." Diário Económico, Maputo, 2025.
- SANTOS, M. R. "*Cibersegurança e governo electrónico: desafios para a protecção de dados sensíveis e a continuidade dos serviços públicos*." Revista Brasileira de Segurança da Informação, v. 8, p. 45–60, 2022.
- SAXENA, Megha. "*Cybercrime in India*." International Journal of Science and Research (IJSR), v. 12, n. 11, nov. 2023.
- SEDENBERG, Elaine M.; DEMPSEY, James X. *Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs*. [S.l.]; 2018
- SEGUNDO, John. *Cybersecurity Governance and Regulatory Challenges in Developing Nations*. London: Routledge, 2015.
- SHAD, Muhammad Riaz. *Cyber security: challenges and the way forward*. Pakistan: National University of Modern Languages (NUML), [s.d.].
- UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *Module 7: National capacity and international cooperation Cybercrime Teaching Module Series*. In: Cybercrime Module 7: Key Issues: National Capacity and International Cooperation. Vienna: UNODC, 2013.

Sites consultados

- https://intic.gov.mz/apresentacao/ acesso em 10 de Julho de 2025
- https://intic.gov.mz/intic-realiza-primeiro-workshop-de-avaliacao-de-riscos-de-seguranca-cibernetica/ acesso em 10 de Julho de 2025
- https://www.diarioeconomico.co.mz/2023/02/15/trends/tech/intic-nao-vamos-acabar-com-ataques-ciberneticos-mas-esperamos-mitiga-los/ acesso em 15 de Julho de 2025

APÊNDICE

Apêndice A: perguntas feitas no INTIC para recolha de dados

A presente pesquisa tem como tema: análise dos ataques cibernéticos no governo electrónico (2020-2023): o caso do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC), o mesmo é realizado como parte da conclusão do curso de Licenciatura em Administração Pública na Universidade Eduardo Mondlane. Os dados colectados serão usados apenas para fins acadêmicos.

Guião de entrevistas para recolha de dados

Análise dos ataques cibernéticos no governo electrónico (2020-2023): o caso do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC),

Entrevistado (a) :_____

Data:_____

Questionário

1. Fale-nos sobre o panorama geral dos ataques cibernéticos em Moçambique.
2. Quais são os principais ataques cibernéticos que se têm registado no e-GOV?
3. Quem são os principais promotores desses ataques?
4. Qual tem sido o papel do INTIC na prevenção e redução desses casos?
5. Quais são as consequências dos ataques cibernéticos no e-GOV?
6. Quais são os desafios do INTIC no combate aos ataques cibernéticos?
7. Como você vê o papel do INTIC no combate aos ataques cibernéticos?
8. Como avalia a eficiência e eficácia operacional do INTIC no combate aos ataques cibernéticos?
9. Quanto a accountability, como o INTIC promove a transparência, a responsabilidade e prestação de contas no combate aos ataques cibernéticos?

Muito obrigado pela sua colaboração.

Apêndice B: perguntas feitas no INAGE para recolha de dados

A presente pesquisa tem como tema: análise dos ataques cibernéticos no governo electrónico (2020-2023): o caso do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC), o mesmo é realizado como parte da conclusão do curso de Licenciatura em Administração Pública na Universidade Eduardo Mondlane. Os dados colectados serão usados apenas para fins académicos.

Guião de entrevistas para recolha de dados

Análise dos ataques cibernéticos no governo electrónico (2020-2023): o caso do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC),

Entrevistado (a) :_____

Data:_____

Questionário

1. Que tipos de ataques cibernéticos têm sido mais frequentes contra sistemas sob gestão do INAGE?
2. O INAGE promove capacitação regular dos seus funcionários em boas práticas de segurança digital?
3. Há campanhas de sensibilização voltadas aos servidores públicos sobre segurança no e-GOV?
4. Quais são os maiores desafios enfrentados pelo INAGE no combate aos ataques cibernéticos?
5. O número de profissionais especializados em cibersegurança dentro do INAGE é suficiente?
6. Os recursos tecnológicos disponíveis são adequados para lidar com ameaças avançadas?

Muito obrigado pela sua colaboração.

ANEXOS

Anexo A: Credencial emitida pela UEM para a solicitação da recolha de dados no INTIC

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE LETRAS E CIÊNCIAS SOCIAIS

CREDENCIAL Nº169/DRA-FLCS/ 2025

No âmbito da disciplina de Trabalho de Fim de Curso, credencia-se junto ao Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC), o Sr. **Alberto António Matsimbe,** estudante do 4º ano do Curso de Licenciatura em Administração Pública, para realizar o trabalho de recolha de dados sobre o tema "Análise dos ataques cibernéticos no E-Gov: o caso do Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC)."

Agradece-se antecipadamente todo o apoio que lhe possa ser prestado para o bom andamento do trabalho.

Maputo, 10 de Junho de 2025

O Director Nacional Adjunto Para área de Graduação

Prof. Doutor Marlino Eugénio Mubai

(Professor Auxiliar)

Anexo B: Credencial emitida pela UEM para a solicitação da recolha de dados no INAGE

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE LETRAS E CIÊNCIAS SOCIAIS

CREDENCIAL Nº 48/DRA-FLCS/ 2025

No âmbito da disciplina de Trabalho de Fim do Curso, credencia-se junto ao Instituto Nacional do Governo Eletrónico, o Sr. **Alberto António Matsimbe**, estudante do 4º ano do Curso de Licenciatura em Administração Pública, para realizar o trabalho de recolha de dados sobre o tema "Análise dos crimes cibernéticos no governo eletrónico em Moçambique (2020- 2023) : o caso do Instituto Nacional do Governo Eletrónico."

Agradece-se antecipadamente todo o apoio que lhe possa ser prestado para o bom andamento do trabalho.

Maputo, 01 de Abril de 2025

O Director Nacional Adjunto Para área de Graduação

Prof. Doutor Marlino Eugénio Mubai

(Professor Auxiliar)

11/04/2025

Anexo C: credencial para recolha de dados

INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

Autoridade Reguladora de TIC

Exmo. Senhor
Prof. Doutor Marlino Eugénio Mubai
Director Nacional Adjunto para Área de Graduação
Faculdade de Letras e Ciências Sociais
Universidade Eduardo Mondlane
MAPUTO

Nota: nº 170/INTIC/PCA/020/2025 Maputo, aos de 20 Agosto de 2025

Assunto: Recolha de Dados

O Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), acusa a recepção da vossa carta datada de 18 de Junho de 2025, através da qual a Faculdade de Letras e Ciências Socias da UEM, solicita ao INTIC, **a favor do Sr. Alberto António Matsimbe** a recolha de dados para elaboração do Trabalho do fim do curso, subordinado ao tema: " ***Análise do ataque cibernético no E-Gov: o caso do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC)".***

É neste contexto que o INTIC aceita ao pedido acima referido, e designa o Engº Eugénio Jeremias, Director da Divisão de Segurança Cibernética e Protecção de Dados para cocrdenar o trabalho deste estudante.

Sem mais de momento, aproveitamos a oportunidade para endereçar os nossos protestos de elevada consideração e respeito.

Prof. Doutor Engº. Lourino Alberto Chemane
Presidente do Conselho de Administração

Rua José Mateus Nº 437; ☎ (258) 21498786/7
E-mail: info@inic.gov.mz URL: www.inic.gov.mz
Maputo, Moçambique