|  |
| --- |
| Descrição: LOGO  **ACADEMIA DE ALTOS ESTUDOS ESTRATÉGICOS**  **CURSO DE ENGENHARIA DE INFORMÁTICA E SEGURANÇA CIBERNÉTICA**  **NARCISO PASCOAL ALBINO CADEADO**  **TÍTULO DO TRABALHO: SUBTÍTULO**  **MALUANA**  **2023** |

|  |
| --- |
| NARCISO PASCOAL ALBINO CADEADO  TÍTULO: E SUBTÍTULO ( se houver, centralizado)  Monografia apresentada à Academia de Altos  Estudos Estratégicos para obtenção do título  de Licenciatura no Curso de Engenharia de  Informática e Segurança-Cibernética.  Supervisores: Prof. Dr. José de Andrade  Mestre Mateus Cardoso  Maluana  2023 |

|  |
| --- |
| 1. Declaro que esta monografia é resultado da minha investigação pessoal e das orientações dos mesu supervisores, o seu conteúdo é original e todas as fontes consultadas esta~o devidamente mencionadas no texto, nas notas e na bibliografia final. Declaro ainda, que este trabalho não foi apresentado em nenhuma outra instituição para a obtenção de qualquer grau académico**”.**  Ficha catalográfica  Rajabo, Maria da Glória  Segurança Cibernética e Protecção de Infraestruturas Críticas em Moçambique: Caso do Banco de Moçambique/Maria da Glória Rajabu; orientador: João António. – Maluana, 2022. 45 f.  Monografia (Licenciatura – Academia de Altos Estudos Estratégicos – AAEE – Licenciatura em Engenharia de Informática e segurança Cibernética  1. Segurança Cibernética. 2. Infraestruturas Críticas. 3. Protecção da Informação.  Maluana  2023 |

Folha de aprovação



**ACADEMIA DE ALTOS ESTUDOS ESTRATÉGICO (AAEE)**

**DIRECÇÃO PEDAGÓGICA**

**SESSÃO DE AVALIAÇÃO DO TRABALHO DE FIM DO CURSO**

O (a) Estudante \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ está convocado (a) à apresentação e defesa oral do seu Trabalho de Fim do Curso, no dia \_\_\_\_\_ do mês \_\_\_\_\_\_ do ano dois mil e \_\_\_\_, pelas \_\_\_\_\_:\_\_\_\_\_\_ horas \_\_\_\_\_, no Campus da AAEE, no auditório/sala n\_\_\_\_.

O Júri:

Presidente: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Assinatura\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Arguente: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Assinatura\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Assinatura\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maluana, aos \_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 20\_\_\_\_

**Dedicatória**

**Resumo**

**Abstract**

**Lista de ilustrações**

**Índice**

[1. CAPÍTULO I - Introdução 10](#_Toc138880629)

[**1.1.** **Contextualização** 10](#_Toc138880630)

[**1.2.** **Descrição do Problema** 11](#_Toc138880631)

[**1.3.** **Justificativa** 12](#_Toc138880632)

[**1.4.** **Objectivos** 13](#_Toc138880633)

[**1.4.1.** **Objectivo Geral** 13](#_Toc138880634)

[**1.4.2.** **Objectivos Especifícos** 13](#_Toc138880635)

[2. CAPÍTULO II- Metodologia 14](#_Toc138880636)

[**2.1.** **Estrutura do trabalho** 14](#_Toc138880637)

[3. CAPÍTULO III- Revisão da Literactura 14](#_Toc138880638)

[**3.1.** **Ataques DDoS** 14](#_Toc138880639)

[**3.2.** **Balanceamento de carga** 14](#_Toc138880640)

[**3.3.** **Arquitetura distribuída** 14](#_Toc138880641)

[**3.4.** **Técnicas de defesa contra DDoS** 14](#_Toc138880642)

[**3.5.** **Sistemas de detecção e monitoramento** 14](#_Toc138880643)

[4. CAPÍTULO IV – Caso de Estudo 15](#_Toc138880644)

[5. CAPÍTULO V- Proposta da Solução 15](#_Toc138880645)

[6. CAPÍTULO VI -Discussão de resultados 15](#_Toc138880646)

[7. CAPÍTULO VII- Conclusões e Recomendações 15](#_Toc138880647)

[**7.1.** **Conclusões** 15](#_Toc138880648)

[**7.2.** **Recomendações** 15](#_Toc138880649)

[8. BIBLIOGRAFIA 15](#_Toc138880650)

[Glossário (opcional) 16](#_Toc138880651)

[Apêndice (opcional) 16](#_Toc138880652)

[Anexo(s) (opcional) 16](#_Toc138880653)

# 1. CAPÍTULO I - Introdução

## **Contextualização**

A Internet revolucionou a forma como as pessoas se comunicam, interagem e acessam informações. Segundo Castells (2001) a tecnologia da informação é o equivalente atual à eletricidade na era industrial.

Ao longo dos anos, a internet evoluiu rapidamente e se tornou uma ferramenta essencial tanto para organizações governamentais, para não governamentais, como também para instituições de ensino e empresas. A internet afeta o funcionamento das organizações governamentais, pois, estas organizações utilizam a internet para serviços públicos online, comunicação interna, coleta de dados e interação com os cidadãos (Chadwick & Philip N., 2009). Da mesma forma, as organizações não governamentais também se beneficiam da internet, de acordo com Kotler (1931 citado por Silva, 2017), a internet oferece novas possibilidades para as empresas conduzirem seus negócios com mais eficiência, pois é possível transmitir muito mais informações de seus produtos.

Face aos benefícios que a conectividade da internet oferece, muitas instituições de ensino e empresas passaram a usar sistemas de computadores para auxiliar e agilizar as suas actividades diárias.

A AAEE[[1]](#footnote-1) é uma das instituições de ensino superior que utiliza de forma massiva os sistemas de computadores para armazenar ficheiros, partilhar ficheiros, comunicação entre outras actividades.

No entanto, com o aumento da conectividade e o volume crescente de dados trafegando pela internet, surgiram desafios relacionados à segurança cibernética e, segundo Schneier (2000), os Governos e instituições sabem da importância de não terem seus segredos militares nas mãos de seus inimigos e, de manterem seus sistemas protegidos contra ataques cibernéticos.

Kevin Mitnick nas obras "The Art of Deception" e "The Art of Deception" mostra que os ataques cibernéticos eram menos sofisticados devido às limitações tecnológicas da época, limitações estas que, não existem actualmente. O custo do Crime Cibernético em 2022 foi de US $ 8.4 trilhões e, os especialistas prevêem que esse número aumentará para US $ 20 trilhões até 2026 (Ahlgren, 2023).

Os ataques cibernéticos têm efeitos devastadores para as organizações, em particular o ataque DDoS[[2]](#footnote-2). Nesse tipo de ataque, os atacantes coordenam computadores para “bombardearem” a máquina alvo com requisições ou dados com a finalidade de deixar a máquina alvo inacessível para utilizadores legítimos (Radware, 2013).

Moçambique, assim como outros países, também tem sofrido ataques Cibernéticos. Vários portais de instituições públicas e governamentais moçambicanas estavam parcialmente inoperacionais no dia 21/02/2022 e, o seu conteúdo foi substituído por uma página que anunciava um ataque informático por "hackers iemenitas” (DW, 2022).

No caso específico da AAEE, segundo algumas informações facultadas pelo gestor principal dos servidores daquela instituição, também tem sofrido tentativas de intrusão frequentemente e que a instituição esta ciente de que precisa criar mecanismos que deixem os sistemas da instituição cada vez mais seguros e resilientes.

Com o exposto acima, o presente trabalho se insere no desenvolvimento de uma Sistema que servirá como mecanismo para mitigar futuros ataques de negação de serviço direcionados as plataformas usadas na AAEE e, deste modo melhorar a resiliência destes e capacidade de lidar com sobrecargas de requisições.

## **Descrição do Problema**

Com vista a fazer face ao crescimento das actividades laborais da AAEE e com o aumento no número de estudantes, surgiu a necessidade de implantação de certas soluções tecnológicas para que, estas soluções pudessem agilizar os processos da AAEE. Os Sistemas que são usadas pela instituição de ensino superior estão implantadas em uma DMZ[[3]](#footnote-3), por questões de segurança. Actualmente os sistemas da instituição são amplamente usados, principalmente, o de Gestão Académica que é responsável pelo progresso académico dos estudantes daquela instituição.

A cada ano a AAEE recebe novos estudantes e com isso, aumenta também a quantidade de dados armazenados. Todos os dados gerados pelos sistemas da instituição permanecem armazenados nos servidores internos da instuição, não existindo assim qualquer outra replica do sistema. <autor que fala> defende que é necessário a existência de uma ou mais replicas do sistema. Segundo …. <Colocar o autor que infatiza sobre a necessidade de se criarem replicas de um sistema como uma medida de segurança>.

Os sistemas da AAEE possuem apenas um ponto de falha, ou seja, na situação de falha de fornecimento de energia, falhas no servidor interno ou até mesmo falta de internet por parte do provedor de internet, todos os sistemas ficam desligados e, as actividades que dependem destes sistemas, ficam afectadas.

A não existência de mecanismos que possibilitam a escalabilidade automática dos sistemas em caso de aumento de demanda, aliado ao facto da arquitetura de implantação usada ser monolítica[[4]](#footnote-4), é um problema de segurança, pois, torna os sistemas da AAEE “alvos fáceis” a um ataque de negação de serviço. De acordo com <> os atacantes que buscam tornar indisponível um determinado sistema tem menos dificuldades em faze-lo em sistemas centralizados, como é o caso da AAEE e, segundo com <Autor> a arquitetura monolítica tem a desvantagem de …

Com os problemas verificados no actual cenário de implantação dos servidores da AAEE, a solução adoptada neste trabalho é o desenvolvimento de um sistema que irá possibilitar a fácil e segura replicação dos sistemas da AAEE para outros servidores confiáveis fora da rede interna, possibilitando assim a escalabilidade, desempenho e resiliência em caso de ataques Cibernéticos de negação de serviço.

## **Justificativa**

A internet actualmente faz parte das actividades desenvolvidas por muitas profissões ao redor do mundo e, a quantidade de pessoas ao redor do mundo que tem usado esta tecnologia aumentou consideravelmente (IstoéDinheiro, 2023). A conectividade tornou-se parte integral do dia-a-dia das pessoas ao redor do mundo, facilitando processos e criando novas oportunidades de negócio. Apesar de todos os benéficos que a internet trouxe, com ela vieram também os problemas de segurança e os ataques cibernéticos. O número de ataques cibernéticos contra instituições cresce a cada ano (Martins, 2023). O ataque de negação de serviço pode causar grandes perdas a instituições por deixa-las inoperantes, fazendo assim com que os funcionários percam horas de trabalho por falta de funcionamento dos sistemas oque consequentemente leva a perda de valores monetários.

Com o exposto acima, é notável a importância de estudos relacionado a ataques de negação de serviço e suas formas de mitigação, pois, estes estudos culminam na aquisição de novos conhecimentos numa altura em que a internet é amplamente usada por muitas instituições moçambicanas. Além disso os ataques de negação de serviço tem sido cada vez mais sofisticados oque exige o estudo continuo na criação de novas formas de mitigação.

Este projecto não só irá beneficiar a AAEE, como também ira beneficiar todas as outras instituições que tem o mesmo problema que a AAEE. Depois de desenvolvida a plataforma poderá ser usada para os sistemas do sector público assim como do sector privado fazendo assim com que os sistemas se tornem resilientes a ataques de negação de serviço.

## **Objectivos**

### **Objectivo Geral**

Desenvolver um sistema de proteção contra ataques de negação de serviço baseado em balanceamento de carga e arquitetura distribuida.

### **Objectivos Especifícos**

* Estudar a arquitetura de implantação dos sistemas da AAEE;
* Identificar os problemas existentes na actual arquitetura de implantação dos sistemas da AAEE;
* Identificar os mecanismos de segurança actualmente usados na AAEE para mitigar ataques de negação de serviço;
* Estudar o funcionamento dos ataques modernos de negação de serviço;
* Realizar testes de segurança;
* Estudar os mecanismos já existentes para mitigação de ataques de negação de serviço;
* Documentar o processo desenvolvimento do novo sistema para mitigar os futuros ataques de negação de serviço contra os sistemas da AAEE;
* Desenvolver um protótipo funcional;
* Realizar testes de usabilidade do protótipo.

# CAPÍTULO II- Metodologia

## **Estrutura do trabalho**

# CAPÍTULO III- Revisão da Literactura

## **Ataques DDoS**

Descreva os diferentes tipos de ataques DDoS, como ataques de negação de serviço distribuídos, ataques de amplificação, ataques de exaustão de recursos, entre outros. Explique as motivações por trás desses ataques e os danos que podem causar às redes e serviços.

## **Balanceamento de carga**

Explique os conceitos e técnicas de balanceamento de carga em sistemas distribuídos. Discuta diferentes algoritmos de balanceamento de carga, como round-robin, ponderação, baseado em desempenho, entre outros. Aborde como o balanceamento de carga pode ser aplicado para mitigar ataques DDoS, distribuindo o tráfego de forma equilibrada entre os sistemas.

## **Arquitetura distribuída**

Descreva os princípios e conceitos da arquitetura distribuída, incluindo a descentralização de recursos, tolerância a falhas e escalabilidade. Explique como uma arquitetura distribuída pode ajudar a lidar com ataques DDoS, distribuindo o tráfego entre vários nós e evitando pontos únicos de falha.

## **Técnicas de defesa contra DDoS**

Explore as diferentes técnicas utilizadas para defender redes e sistemas contra ataques DDoS. Isso pode incluir filtragem de pacotes, detecção e mitigação de anomalias de tráfego, uso de sistemas de reputação de IP, técnicas de rate limiting, entre outras abordagens.

## **Sistemas de detecção e monitoramento**

Aborde os sistemas e ferramentas de detecção e monitoramento utilizados para identificar ataques DDoS em tempo real. Descreva técnicas de análise de tráfego, detecção de padrões e comportamentos anormais, além de sistemas de alerta para notificar sobre possíveis ataques.

# CAPÍTULO IV – Caso de Estudo

# CAPÍTULO V- Proposta da Solução

# CAPÍTULO VI -Discussão de resultados

# CAPÍTULO VII- Conclusões e Recomendações

## **Conclusões**

## **Recomendações**

# BIBLIOGRAFIA

ANEXO III: ELEMENTOS PÓS-TEXTUAIS

# Glossário (opcional)

É uma relação, em ordem alfabética, de palavras ou expressões de uso restrito ou pouco conhecidos, acompanhadas das respectivas definições, com o objetivo de esclarecer o leitor sobre o significado dos termos empregados no trabalho. O glossário é um título sem indicativo numérico, ou seja, não possui identificação numérica como as outras secções, portanto, o título deve estar centralizado e negritado no texto.

# Apêndice (opcional)

São textos ou documentos elaborados pelo autor, a fim de complementarem sua argumentação, sem prejuízo da unidade nuclear do trabalho. Podem-se incluir nos apêndices: questionários de pesquisas, tabulação de dados, ilustrações e outros documentos preparados pelo autor.

Sua paginação deve ser contínua a do texto. Os Apêndices devem ser identificados por inicial a letra maiúsculas, seguidas de travessão e dos respectivos títulos. Se tiver apenas um apêndice use apenas o rótulo ‘Apêndice’, se possui dois ou mais, rotule cada um com uma letra maiúsculas na ordem como são mencionados no texto: ‘Apêndice A’, ‘Apêndice B’, etc. Cada apêndice deve ter um título e no texto deve ser citado por seus rótulos.

*Modelo de apêndice*

|  |
| --- |
| Apêndice A – Instrumento de Coleta de Dados  Apêndice B – Análise da demanda máxima |

# Anexo(s) (opcional)

São documentos não elaborados pelo autor, que servem de fundamentação, comprovação ou ilustração à parte nuclear do trabalho.

Podem-se incluir nos anexos: leis, ilustrações e outros documentos não elaborados pelo autor. Sua paginação deve ser contínua a do texto. O título ‘Anexo’ deve aparecer com a inicial maiúscula e as demais minúsculas centralizado. Se tiver apenas um anexo use apenas o rótulo ‘Anexo’, se possui dois ou mais, rotule cada um com uma letra maiúsculas na ordem como são mencionados no texto: ‘Anexo A’, ‘Anexo B’, etc. Cada anexo deve ter um título e no texto deve ser citado por seus rótulos.

1. AAEE - Académia de Altos Estudos Estratégicos. [↑](#footnote-ref-1)
2. DDoS - Distributed Denial-of-Service. [↑](#footnote-ref-2)
3. DMZ [↑](#footnote-ref-3)
4. [↑](#footnote-ref-4)