REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

AVALIAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB CRÍTICAS: UM ESTUDO DE CASO BASEADO EM TESTES DE PENETRAÇÃO

VULNERABILITY ASSESSMENT OF CRITICAL WEB APPLICATIONS: A CASE STUDY BASED ON PENETRATION TESTING

Ciências Exatas e da Terra, Engenharias • 13/08/2026

REGISTRO DOI: 10.70773/revistatopicos/786502097

Julião Artur Mussa[1]

Nelson Flores Ambrique[2]

Zefanias Álvaro Mobiua[3]

Joaquim Jaime Fagir[4]

Bráulio Sebastião André[5]

RESUMO

As aplicações web desempenham um papel fundamental na gestão de processos organizacionais e no armazenamento de informações sensíveis. Contudo, a crescente sofisticação das ameaças cibernéticas torna indispensável a realização de avaliações periódicas de segurança. Este estudo apresenta uma análise de vulnerabilidades realizada numa aplicação web institucional por meio de técnicas de testes de penetração. A investigação adotou uma abordagem aplicada e qualitativa, baseada nas fases de reconhecimento, mapeamento, análise e validação de vulnerabilidades. Os resultados permitiram identificar falhas críticas relacionadas com configurações inseguras, mecanismos de autenticação inadequados e controlos de acesso insuficientes, com destaque para a vulnerabilidade de Referência Direta Insegura a Objetos (IDOR). As vulnerabilidades observadas demonstram potencial para comprometer a confidencialidade, integridade e disponibilidade da informação. Com base nos resultados obtidos, são propostas medidas de mitigação alinhadas às boas práticas internacionais de segurança da informação e ao framework OWASP. O estudo contribui para o fortalecimento da segurança de aplicações web críticas e fornece orientações para a melhoria da gestão de riscos cibernéticos em ambientes institucionais.

Palavras-chave: Segurança da Informação; Testes de Penetração; Vulnerabilidades Web; OWASP; Gestão de Riscos.

ABSTRACT

Web applications play a fundamental role in managing organizational processes and storing sensitive information. However, the increasing sophistication of cyber threats makes periodic security assessments indispensable. This study presents a vulnerability analysis conducted on an institutional web application

using penetration testing techniques. The research adopted an applied, qualitative, and descriptive approach, structured around the phases of reconnaissance, mapping, vulnerability analysis, and validation. The results enabled the identification of critical flaws related to insecure configurations, inadequate authentication mechanisms, and insufficient access controls, with particular emphasis on the Insecure Direct Object Reference (IDOR) vulnerability. The observed vulnerabilities demonstrate the potential to compromise the confidentiality, integrity, and availability of information. Based on the findings, mitigation measures aligned with international information security best practices and the OWASP framework are proposed. This study contributes to strengthening the security of critical web applications and provides guidance for improving cyber risk management in institutional environments.
Keywords: Information Security; Penetration Testing; Web Vulnerabilities; OWASP; Risk Management.

1. INTRODUÇÃO

A crescente transformação digital das organizações tem impulsionado a adoção de aplicações web para suporte a processos administrativos, financeiros e operacionais. Estas aplicações assumem um papel estratégico ao centralizarem informações críticas e permitirem a prestação de serviços digitais a diferentes grupos de utilizadores. Contudo, a expansão da superfície de ataque associada à crescente conectividade dos sistemas tem aumentado significativamente os riscos relacionados com a segurança da informação.

Nos últimos anos, os incidentes de cibersegurança envolvendo aplicações web tornaram-se uma das principais preocupações das organizações públicas e privadas. Vulnerabilidades relacionadas com falhas de autenticação, configurações inseguras, controlo inadequado de acessos e exposição indevida de dados continuam a figurar entre as ameaças mais exploradas por atacantes, conforme evidenciado pelos relatórios do *Open Web Application Security Project* (OWASP) e por diversos estudos recentes na área da segurança de aplicações.

Apesar da ampla adoção de mecanismos tradicionais de proteção, como firewalls, sistemas de deteção de intrusão e soluções de antivírus, muitas organizações ainda apresentam fragilidades que apenas podem ser identificadas através de abordagens proativas de avaliação de segurança. Neste contexto, os testes de penetração (*penetration testing*) constituem uma metodologia amplamente reconhecida para a identificação, validação e priorização de vulnerabilidades em ambientes computacionais reais, permitindo simular o comportamento de potenciais atacantes e avaliar o impacto efetivo das falhas encontradas.

Embora existam diversos estudos sobre vulnerabilidades em aplicações web, observa-se uma escassez de investigações que documentem evidências empíricas obtidas através de avaliações práticas em ambientes institucionais reais, particularmente em contextos organizacionais de países em desenvolvimento. Esta lacuna limita a compreensão dos desafios enfrentados pelas organizações na implementação de mecanismos eficazes de proteção dos seus ativos digitais.

Diante deste cenário, o presente estudo tem como objetivo avaliar vulnerabilidades de segurança numa aplicação web crítica por meio da utilização de técnicas de testes de penetração, identificando fragilidades relacionadas com autenticação, controlo de acesso e configurações de segurança. Adicionalmente, procura-se analisar os potenciais impactos dessas vulnerabilidades sobre os princípios da confidencialidade, integridade e disponibilidade da informação, bem como propor medidas de mitigação alinhadas às melhores práticas internacionais de cibersegurança.

A principal contribuição deste trabalho consiste na apresentação de evidências empíricas obtidas através de uma avaliação prática de segurança, demonstrando como vulnerabilidades aparentemente simples podem comprometer ativos digitais críticos e gerar riscos significativos para a continuidade operacional e para a proteção da informação organizacional.

O artigo encontra-se estruturado da seguinte forma: a Secção 2 apresenta a fundamentação teórica; a Secção 3 descreve a metodologia adotada; a Secção 4 apresenta e discute os resultados obtidos; e a Secção 5 apresenta as conclusões, limitações e recomendações para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Segurança da Informação e Proteção de Ativos Digitais

A transformação digital tem ampliado significativamente a dependência das organizações em sistemas de informação e aplicações web para suporte às suas operações críticas. Neste contexto, a segurança da informação assume um papel estratégico

na proteção dos ativos digitais, garantindo a continuidade dos serviços e a proteção dos dados organizacionais.

Segundo a norma ISO/IEC 27001:2022, a segurança da informação deve ser gerida através de uma abordagem sistemática baseada em risco, assegurando a proteção da confidencialidade, integridade e disponibilidade da informação. Estes três princípios, conhecidos como Tríade CIA (*Confidentiality, Integrity and Availability*), constituem a base conceptual da maioria dos modelos contemporâneos de gestão da segurança da informação.

A violação de qualquer destes princípios pode resultar em impactos operacionais, financeiros, legais e reputacionais para as organizações. A norma ISO/IEC 27001:2022 estabelece requisitos para a implementação de Sistemas de Gestão da Segurança da Informação (SGSI), enquanto a ISO/IEC 27002:2022 fornece orientações detalhadas para a seleção, implementação e monitorização de controlos de segurança.

2.2. Governança de Segurança e Gestão de Riscos

A segurança da informação deixou de ser exclusivamente uma questão tecnológica para assumir uma dimensão estratégica de governança organizacional. O COBIT 2019 (*Control Objectives for Information and Related Technologies*) fornece um modelo abrangente de governança e gestão de tecnologia da informação, permitindo que as organizações alinhem os investimentos em TI com os seus objetivos estratégicos, enfatizando a gestão de riscos e a conformidade regulatória.

Complementarmente, o *NIST Cybersecurity Framework* (CSF) 2.0 propõe uma abordagem estruturada baseada em funções

fundamentais: identificar, proteger, detetar, responder e recuperar face a ameaças cibernéticas, introduzindo explicitamente a função *Govern* para reconhecer a necessidade de integração da cibersegurança nos mecanismos de governança organizacional. A combinação entre COBIT 2019, ISO/IEC 27001:2022 e NIST CSF 2.0 permite às organizações desenvolver uma abordagem holística para a gestão dos riscos digitais.

2.3. Vulnerabilidades em Aplicações Web

As aplicações web representam atualmente uma das principais superfícies de ataque exploradas por agentes maliciosos devido à sua ampla exposição à Internet e ao elevado volume de dados sensíveis processados. Uma vulnerabilidade pode ser definida como uma fraqueza existente em sistemas, aplicações ou processos que pode ser explorada por uma ameaça para comprometer os objetivos de segurança.

De acordo com a ISO/IEC 27002:2022, as organizações devem implementar processos contínuos de identificação, avaliação, tratamento e monitorização de vulnerabilidades, assegurando que os riscos sejam mantidos dentro de níveis aceitáveis através de avaliações proativas.

2.4. Testes de Penetração Como Instrumento de Avaliação de Segurança

Os testes de penetração (Penetration Testing) são utilizados para avaliar a eficácia dos mecanismos de segurança implementados em sistemas de informação através da simulação de ações executadas por potenciais atacantes. Segundo Weidman (2014), esta abordagem estruturada envolve fases sequenciais e interdependentes que

compreendem a preparação e definição do escopo legal, a recolha de informações (*information-gathering*), a modelação de ameaças, a análise técnica de vulnerabilidades, a exploração controlada das falhas encontradas, a pós-exploração (para determinar o valor real dos sistemas comprometidos) e, por fim, a geração de relatórios detalhados contendo as recomendações de mitigação.

2.5. OWASP Top 10 e Segurança de Aplicações Web

O *Open Web Application Security Project* (OWASP) constitui uma das principais iniciativas globais dedicadas à melhoria da segurança de software. O OWASP Top 10 é amplamente reconhecido como a referência internacional para a identificação dos riscos mais críticos que afetam aplicações web. Na sua versão mais recente (OWASP Top 10:2021), o framework reestruturou as suas categorias para refletir a evolução do cenário de ameaças modernas.

Entre as categorias definidas, destacam-se: *A01:2021 – Broken Access Control* (que agrupa falhas de autorização e isolamento de dados, incluindo as Referências Diretas Inseguras a Objetos - IDOR); *A02:2021 – Cryptographic Failures*; *A03:2021 – Injection*; *A04:2021 – Insecure Design*; *A05:2021 – Security Misconfiguration*; *A06:2021 – Vulnerable and Outdated Components*; *A07:2021 – Identification and Authentication Failures*; *A08:2021 – Software and Data Integrity Failures*; *A09:2021 – Security Logging and Monitoring Failures*; e *A10:2021 – Server-Side Request Forgery (SSRF)*. No âmbito deste estudo, as falhas de controlo de acesso (A01), configuração de segurança (A05) e identificação/autenticação (A07) assumem especial relevância devido à sua frequência e severidade em ambientes institucionais.

3. METODOLOGIA

3.1. Natureza da Pesquisa

O presente estudo caracteriza-se como uma investigação aplicada, de natureza qualitativa e caráter descritivo, configurando-se como um estudo de caso estruturado. A abordagem aplicada justifica-se pela finalidade prática de diagnosticar e propor mitigações para um ambiente computacional real, enquanto a vertente qualitativa e descritiva reside na análise interpretativa e caracterização sistemática do impacto das falhas descobertas sobre a segurança da informação institucional.

3.2. Ambiente de Estudo

O estudo foi conduzido numa aplicação web institucional considerada crítica para o suporte de processos organizacionais, que disponibiliza funcionalidades de autenticação, processamento de dados sensíveis e emissão de relatórios/fichas financeiras. Por razões éticas, de confidencialidade e de divulgação responsável de vulnerabilidades (*responsible disclosure*), a identidade da organização e a URL da plataforma foram estritamente preservadas.

3.3. Estratégia de Avaliação

A avaliação adotou a metodologia de Teste de Penetração do tipo *Black-Box* (Caixa-Preta). Nesta modalidade, os avaliadores simularam a perspetiva de um atacante externo posicionado na Internet, operando sem qualquer conhecimento prévio sobre o código-fonte, a arquitetura de rede interna, a documentação do sistema ou credenciais de acesso privilegiadas.

3.4. Procedimentos de Recolha e Análise de Dados

A execução técnica dos testes seguiu o processo metodológico estruturado em quatro fases principais:

- **Fase 1 – Reconhecimento:** Recolha passiva e ativa de informações públicas sobre a aplicação para identificar a superfície de exposição, servidores web utilizados e tecnologias associadas sem interações invasivas.

- **Fase 2 – Mapeamento e Enumeração:** Identificação ativa de diretórios expostos, componentes acessíveis, módulos de relatórios e vetores de entrada de dados suscetíveis a falhas lógicas e de configuração.

- **Fase 3 – Análise de Vulnerabilidades:** Execução combinada de ferramentas automatizadas e testes manuais exaustivos direcionados à validação de mecanismos de autenticação, gestão de sessões, consistência de parâmetros em URLs e controlos de autorização no lado do servidor.

- **Fase 4 – Validação e Classificação dos Resultados:** Tentativa de exploração controlada e não destrutiva para eliminação de falsos positivos. As vulnerabilidades confirmadas foram classificadas de acordo com o nível de severidade e mapeadas em conformidade com o framework OWASP Top 10 (2021).

3.5. Considerações Éticas

A investigação foi estritamente pautada pelos preceitos éticos da segurança ofensiva. Os testes foram executados sem causar a negação de serviços (DoS) ou a corrupção de dados operacionais.

Relatórios detalhados contendo as provas de conceito e recomendações técnicas foram formalmente entregues à administração da instituição antes da redação científica deste artigo, mitigando o risco de exploração maliciosa.

4. RESULTADOS E DISCUSSÃO

4.1. Visão Geral dos Resultados

A avaliação de segurança permiteu identificar fragilidades críticas na aplicação web institucional. A classificação das vulnerabilidades validadas foi estruturada com base no framework OWASP Top 10 (2021), conforme sistematizado na Tabela 1.

Tabela 1. Classificação das vulnerabilidades identificadas segundo o OWASP Top 10 (2021)

Categoria OWASP 2021	Nível de Risco	Impacto Potencial
A01:2021 – Broken Access Control (Ex: IDOR)	Crítico	Acesso não autorizado a recursos e exfiltração de dados
A02:2021 – Cryptographic Failures	Crítico	Comprometimento da confidencialidade de dados sensíveis
A07:2021 – Identification and Authentication Failures	Alto	Comprometimento de credenciais e usurpação de sessões
A05:2021 – Security Misconfiguration	Médio	Exposição de informações técnicas e ampliação da superfície de ataque

Fonte: Adaptado de OWASP Top 10 (2021)

Os resultados evidenciam que as ameaças mais severas se concentram na lógica de autorização e proteção de dados, corroborando a tendência global estabelecida pelo OWASP, que posiciona o *Broken Access Control* como a categoria mais prevalente e perigosa em sistemas corporativos modernos.

4.2. Vulnerabilidades Relacionadas com Configuração de Segurança (A05:2021)

A análise revelou a existência de fragilidades associadas à configuração de componentes da infraestrutura e servidores web. Observou-se a persistência de parâmetros padrão e a exposição indevida de diretórios de monitoramento técnico.

Conforme discutido por Khan, Ahmed e Alqahtani (2024), falhas de *Security Misconfiguration* operam frequentemente como um facilitador de alto valor nas fases iniciais de um ataque, fornecendo metadados e informações de infraestrutura que reduzem o esforço do atacante na customização de exploits direcionados. Estes resultados reforçam a necessidade premente de processos de *hardening* contínuos, tal como preconizado pela norma ISO/IEC 27002:2022.

4.3. Vulnerabilidades de Autenticação e Gestão de Credenciais (A07:2021)

Foram identificadas fragilidades nos mecanismos de validação de identidades, caracterizadas por políticas permissivas de palavras-passe e pela ausência de controlos de limitação de tentativas de acesso (*rate limiting*) contra os pontos de autenticação. A ausência de defesas contra ataques automatizados de força bruta valida as preocupações de Khan et al. (2024), que apontam a autenticação

frágil como um dos vetores de comprometimento mais céleres em ecossistemas institucionais.

A mitigação destas falhas exige a transição para modelos robustos que contemplem políticas estritas de complexidade de credenciais e a obrigatoriedade de autenticação multifator (MFA).

4.4. Vulnerabilidades de Controlo de Acesso (A01:2021)

As falhas de controlo de acesso representaram o cenário de maior gravidade descoberto no ambiente de estudo. A aplicação demonstrou falhas severas na segregação de privilégios, permitindo que utilizadores comuns acedessem a rotas e objetos restritos do sistema sem a devida validação de escopo no lado do servidor.

Os resultados convergem diretamente com os alertas de Patel, Singh e Sharma (2023) e Yadav, Kumar e Gupta (2024), que reiteram que a complexidade na implementação de matrizes de autorização em sistemas web modernos tem gerado lacunas onde a identidade do requisitante é assumida como legítima pelo simples facto de estar autenticado, sem validar se a entidade possui permissão explícita para o objeto solicitado.

4.5. A Gravidade das Referências Diretas Inseguras a Objetos (IDOR)

No âmbito das falhas de controlo de acesso (*A01:2021*), os testes manuais revelaram uma vulnerabilidade crítica de IDOR (*Insecure Direct Object References*) localizada especificamente nos módulos de geração de relatórios. Constatou-se que a aplicação expõe identificadores numéricos sequenciais diretamente nos parâmetros

da URL para a requisição de arquivos PDF (como fichas académicas e faturas financeiras).

A ausência de uma rotina de verificação de propriedade do objeto no servidor permitiu que, através da manipulação sequencial destes IDs, os avaliadores acedessem a documentos pertencentes a terceiros.

A implicação institucional deste vetor é severa. A capacidade de automatizar o descarregamento de milhares de registos permite que um agente malicioso:

1. **Mapeie o Rendimento Institucional:** Através da exfiltração em larga escala de faturas e recibos, torna-se viável auditar externamente o fluxo de caixa e a saúde financeira da instituição.

2. **Maximize o Potencial de Engenharia Social:** O acesso a dados detalhados (nomes completos, documentos de identidade, cursos e históricos) viabiliza a criação de campanhas altamente direcionadas de *spear-phishing* contra a comunidade institucional.

3. **Incorra em Desconformidade Legal:** A exposição massiva de dados financeiros e pessoais viola diretamente as diretrizes contemporâneas de proteção de dados, sujeitando a organização a severas sanções legais, litígios por quebra de custódia e danos irreparáveis à reputação pública.

4.6. Implicações para a Governança Digital e Gestão de Riscos

A análise integrada dos resultados demonstra que a remediação das falhas identificadas transcende a esfera puramente técnica. Sob a perspetiva da ISO/IEC 27001:2022 e do framework COBIT 2019, a persistência de credenciais previsíveis e falhas de design como o IDOR funcionam como indicadores de uma governança de TI que necessita de amadurecimento e alinhamento estratégico.

A gestão operacional de riscos, conforme estruturada no *NIST Cybersecurity Framework* 2.0, exige que as organizações não dependam exclusivamente de defesas perimetrais passivas. Os resultados práticos deste estudo de caso evidenciam que a segurança deve ser integrada ao ciclo de vida do desenvolvimento de software (*DevSecOps*), garantindo que controlos lógicos de acesso sejam validados nativamente em cada endpoint da aplicação.

5. CONCLUSÕES, LIMITAÇÕES E TRABALHOS FUTUROS

5.1. Conclusões

Este estudo cumpriu o objetivo de avaliar as vulnerabilidades de segurança de uma aplicação web crítica através de testes de penetração *Black-Box*, mapeando falhas associadas às categorias mais críticas do framework OWASP Top 10 (2021). Os resultados empíricos confirmaram que a ausência de controlos rigorosos de validação de acesso no lado do servidor (como demonstrado no caso do IDOR) e as configurações incorretas de infraestrutura oferecem riscos severos à confidencialidade e integridade dos dados organizacionais.

Os resultados validam empiricamente as estatísticas globais do *Verizon Data Breach Investigations Report* (DBIR) 2025,

evidenciando que falhas lógicas e erros de configuração continuam a figurar como os principais catalisadores de incidentes cibernéticos internacionais. Conclui-se que o teste de penetração periódico atua como um instrumento indispensável de governança, fornecendo a visibilidade proativa necessária para que os gestores de TI possam antecipar-se a ameaças reais e fortalecer de forma contínua a resiliência cibernética institucional.

5.2. Limitações do Estudo

Reconhece-se como limitação o facto de a investigação ter sido circunscrita a uma única aplicação web de uma única instituição, o que impede a generalização estatística dos resultados para outros cenários. Adicionalmente, a abordagem *Black-Box* limitou a análise à superfície externa do sistema; falhas estruturais profundas ao nível do código-fonte (*Source Code Review*) ou vulnerabilidades na arquitetura interna de banco de dados não puderam ser escrutinadas nesta modalidade.

5.3. Trabalhos Futuros

Para investigações futuras, recomenda-se o desenvolvimento de estudos de caso múltiplos e comparativos, englobando diferentes plataformas do setor público e privado para traçar um panorama de maturidade regional em segurança de software. Sugere-se a incorporação do sistema de pontuação quantitativa *Common Vulnerability Scoring System* (CVSS) para enriquecer a priorização de riscos, bem como a avaliação da eficácia da Inteligência Artificial aplicada à deteção precoce de falhas lógicas de controlo de acesso. Por fim, propõe-se a realização de estudos longitudinais que

acompanhem o ciclo de remediação das falhas para aferir o custo-benefício das mitigações aplicadas pelas organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRESS, Jason. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. 3. ed. Amsterdam: Syngress, 2019.

BALOCH, Rafay. Ethical hacking and penetration testing guide. Boca Raton: CRC Press, 2015.

CENTER FOR INTERNET SECURITY. CIS Controls Version 8.1. East Greenbush: CIS, 2024.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION (ISO/IEC). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION (ISO/IEC). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.

ISACA. COBIT 2019 Framework: Governance and Management Objectives. Schaumburg: ISACA, 2019.

KHAN, R.; AHMED, S.; ALQAHTANI, F. Security challenges and mitigation strategies in modern web applications. Computers & Security, Amsterdam: Elsevier, v. 137, p. 103642, 2024. DOI: 10.1016/j.cose.2023.103642.Acesso em: 20 jun. 2026.

KOMAN, J.; JANISZEWSKI, M. SCAnME - scanner comparative analysis and metrics for evaluation. International Journal of Information Security, v. 24, n. 3, 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Cybersecurity Framework (CSF) 2.0. Gaithersburg: U.S. Department of Commerce, 2024. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 20 jun. 2026.

OWASP FOUNDATION. OWASP Top 10: The Ten Most Critical Web Application Security Risks. 2021. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 27 jun. 2026.

SOMMESTAD, T.; HALLBERG, J.; LUNDHOLM, K.; BENGTSSON, J. Variables influencing information security policy compliance: a systematic review. Information & Computer Security, v. 30, n. 2, p. 240–260, 2022.

STUTTARD, Dafydd; PINTO, Marcus. The web application hacker's handbook: finding and exploiting security flaws. 2. ed. Indianapolis: Wiley, 2011.

STUTTARD, Dafydd; PINTO, Marcus. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2. ed. Indianápolis: Wiley, 2011. 912 p.

VERIZON. 2025 Data Breach Investigations Report (DBIR). New York: Verizon Enterprise, 2025.

WEIDMAN, Georgia. Penetration testing: a hands-on introduction to hacking. San Francisco: No Starch Press, 2014.

ZALEWSKI, Michal. The Tangled Web: A Guide to Securing Modern Web Applications. São Francisco: No Starch Press, 2011. 320 p.

---

[1] Docente da Universidade Rovuma, Cidade de Nampula, Moçambique. E-mail: acesse o artigo original para visualizar o e-mail

[2] Discente do Curso de Mestrado em Sistemas de Informação, na Academia Militar, Cidade de Nampula, Moçambique. E-mail: acesse o artigo original para visualizar o e-mail

[3] Discente do Curso de Doutoramento em Tecnologias e Sistemas de Informação da Universidade Pedagógica de Maputo, Cidade de Maputo, Moçambique. E-mail: acesse o artigo original para visualizar o e-mail

[4] Discente do Curso de Doutoramento em Tecnologias e Sistemas de Informação da Universidade Pedagógica de Maputo, Cidade de Maputo, Moçambique. E-mail: acesse o artigo original para visualizar o e-mail

[5] Pós-doc | Universidade de São Paulo, Brasil. E-mail: acesse o artigo original para visualizar o e-mail