POLITÉCNICO DE SANTARÉM
UIIPS – IMPACT SCIENCE

11 - 4 | 2023

Riscos cibernéticos no dia-a-dia do tribunal administrativo: como prevenir?

Cyber risks in the day-to-day of the administrative tribunal: how to prevent them?

Almeida Agostinho Chirindza | Dénice Paulo Jamo | José Estêvão Muagura

Versão eletrónica

URL: https://revistas.rcaap.pt/uiips/ ISSN: 2182-9608

Data de publicação: 31-12-2023 Páginas: 9

Editor

Revista UI_IPSantarém

Referência eletrónica

Chirindza, A.; Jamo, D. & Muagura, J. (2023). Riscos cibernéticos no dia-a-dia do tribunal administrativo: como prevenir? *Revista da UI_IPSantarém*. Número Especial: IV Conferência Intercontinental em Transformação Digital 2023, *11*(4), 24-32. https://doi.org/10.25746/ruiips.v11.i4.34102

revistauiips@ipsantarem.pt
Complexo Andaluz,
Apartado 279
2001-904 Santarém

Revista da UI_IPSantarém – Unidade de Investigação do Instituto Politécnico de Santarém,
Vol. 11, N. º 4, 2023, pp. 24-32, Santarém
ISSN: 2182-9608
https://revistas.rcaap.pt/uiips/

RISCOS CIBERNÉTICOS NO DIA-A-DIA DO TRIBUNAL ADMINISTRATIVO: COMO PREVENIR?

Cyber risks in the day-to-day of the administrative tribunal: how to prevent them?

Almeida Agostinho Chirindza
Instituto Superior Mutassa, Moçambique
aacilenesa@gmail.com

Dénice Paulo Jamo
Instituto Superior Mutassa, Moçambique
shakespearslawyer@gmail.com

José Estêvão Muagura
Instituto Superior Mutassa, Moçambique
joesmuagura@gmail.com

RESUMO

O presente estudo circunscreve-se na reflexão sobre os riscos cibernéticos associados ao uso dos sistemas de informação e comunicação no Tribunal Administrativo em Moçambique no seu dia-a-dia. Para o efeito, recorreu aos métodos mistos para a interpretação dos dados obtidos através do inquérito por questionário e apuramento de resultados por meio de comparação derivada do acervo bibliográfico e documental diverso. O estudo concluíu que o TA funciona na base de diversos sistemas padronizados para a realização das suas distintas atribuições pelo que, reside um conjunto de riscos cibernéticos relacionados com o armazenamento de dados em servidores locais, ataques recorrentes pelo *malwares* e spywares e uso de Microsoft office 2013 bastante desatualizado. Daí que, constituem medidas de mitigação destes riscos a emigração do armazenamento de dados em servidores físicos locais para a nuvem de acesso remoto, atualização do Microsoft office 2013 para Microsoft 365, definição de rúbricas para investigação e reparação localmente de sistemas obstruídos ou infetados por ataques, massificação de treinamentos e consciencialização dos colaboradores sobre matérias relacionadas com riscos cibernéticos, monitoria dos planos de manutenção permanente dos equipamentos e observação das regras internas de uso dos equipamentos informáticos.

Palavras-chave: Risco Cibernético. Informação. Comunicação e Mitigação

ABSTRACT

The present study focuses on the reflection on cyber risks associated with the use of information and communication systems in the Administrative Court in Mozambique in its daily life. To this end, it used mixed methods to interpret the data obtained through the questionnaire survey and to find the results through a comparison of the diverse bibliographic and documentary collection. The study concluded that the TA operates on the basis of several standardised systems to carry out its different tasks, and therefore, there is a set of cyber risks related to data storage on local servers, recurrent attacks by malware and *spyware* and the use of *Microsoft Office* 2013 which is quite outdated. Therefore, measures to mitigate these risks are the emigration of data storage on local physical servers to the remote access cloud, updating *Microsoft office* 2013 to *Microsoft* 365, defining items for investigating and repairing locally obstructed systems or infected by attacks, mass training and awareness of employees on matters related to cyber risks, monitoring of permanent equipment maintenance plans and observing internal rules for the use of computer equipment.

Keywords: Cyber risk. Information. Communication and Mitigation

1 INTRODUÇÃO

"A era digital coloca países de todo o mundo perante um novo conceito de segurança, o de segurança cibernética, que deve ser encarado com responsabilidade e envolvimento de todas as forças vivas da sociedade" (n.º 1, da Resolução n.º 69/2021de 31 de Dezembro) e Moçambique não é uma exceção. Pelo que, a gestão segura dos dados é atualmente imprescindível para o sucesso de qualquer organização, e isso abrange desde informações pessoais de clientes, fornecedores e colaboradores até dados confidenciais relacionados às operações internas (Maluf, 2023).

A crescente conectividade no mundo e dependência da tecnologia aumentou significativamente os riscos cibernéticos, daí a necessidade das organizações estarem atentas e investirem em uma segurança robusta para a sua proteção e segurança. Nesse contexto, a exposição aos riscos cibernéticos requer um monitoramento constante, pois, um simples vazamento pode ter um impacto negativo significativo no negócio, tanto em termos jurídicos, financeiros, ambientais e em outras áreas do saber e de atuação profissionalizante, visto que, a segurança institucional chama uma reputação e amparo da organização.

Este trabalho de pesquisa procura explorar e refletir sobre os riscos cibernéticos associados aos sistemas de informação e comunicação em uso no Tribunal Administrativo (TA) no seu quotidiano, suas características e estratégia de mitigação.

Para a materialização deste objetivo, o trabalho apresenta além da descrição da metodologia em uso, elenca os conceitos operacionais que se debruçam sobre a Tecnologia, perigo, vulnerabilidade, risco, sistema de risco, bacia de risco e riscos cibernéticos na sua plenitude conceptual e caracterização de riscos, descrição do local de estudo, discussão dos resultados, medidas de mitigação e apuramento de conclusões.

2 ENQUANDRAMENTO TEÓRICO/ ESTADO DA ARTE

A materialização da pesquisa foi descrita pelo entrosamento da mobilidade e imobilidade do risco cibernético, associado e alinhavado a sua complexidade do dia-a-dia no Tribunal Administrativo (TA), trazendo técnicas de como esta entidade previne ou transfigura a ótima utilização dos equipamentos informáticos no espaço cibernético e como desvia o risco tecnológico e a respetiva perigosidade. A reflexão deste estudo observou a técnica operacional (conceito) do perigo, risco, vulnerabilidade, tecnologia entre outros termos da complexidade cibernética.

No que respeita a avaliação do impacto do risco cibernético no dia-a-dia no TA, foram utilizados dados recolhidos através do inquérito por questionário aberto aplicado aos diversos técnicos da Direção de Sistema de Informação do TA adstritos aos Departamentos de Sistema de Informação e de Infraestruturas e Redes.

Para a realização desta pesquisa foi utilizado o método misto (indutivo e dedutivo) que se versou na reflexão do risco cibernético, através do dialogo ou entrevista com os técnicos dos Departamentos de Sistema de Informação e de Infraestruturas e Redes, adiante consultas em acervo bibliográfico para o enriquecimento teórico, pois, para a visualização do impacto da ocorrência dos ataques cibernéticos foi estritamente necessário o levantamento das abordagens qualitativa e quantitativa, visto que, a abordagem qualitativa remete a abordagem do ambiente de elementos existentes, estudados e a interpretação de fenómenos e situações, conforme Coutinho (2013). Este autor afirma que esta abordagem vincula indissociavelmente entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números, de modo que o pesquisador tende a analisar dados de forma indutiva, contudo, para transfigurar a linhagem do risco cibernético foi necessário transcrever os créditos da abordagem quantitativa, por meio de dados em números e traduzi-los no meio ou contexto tecnológico. Quanto a tipologia de estudo de caso, optou-se pela pesquisa mista.

3 CONCEITOS OPERACIONAIS

Atualmente a tecnologia está perfeitamente consolidada no dia-a-dia das pessoas assim como no funcionamento de qualquer organização. É impossível ficar alheio à massificação dos aparelhos tecnológicos, à informatização dos dados e ao funcionamento em rede (Santos, 2015) daí que, Lima & da Silva (2012) citando Bueno (1999, p.81), realça que tecnologia é "...um processo contínuo através do qual a humanidade molda, modifica e gera a sua qualidade de vida para possuir a capacidade de se comunicar pela linguagem e habilidade de fabricar utensílios pela técnica." Daí que, o estudo da tecnologia prenuncia a análise das vulnerabilidades que dentre outros fenómenos associam-se a riscos. Cutter (2011), Amaro (2005), analisam a vulnerabilidade como um potencial para perda de acordo com a perigosidade e circunstâncias envolventes ao ambiente tecnológico.

Nas tecnologias, os riscos podem ocorrer de forma interliga a outros no tempo e/ou no espaço envolvendo outros sistemas e plataformas operacionais causando um sistema e uma bacia de riscos caracterizando-se pela conectividade entre a causa e os efeitos. Neste contexto, a ocorrência de uma bacia de riscos é provável a partir do momento em que não apenas se prevê a instalação do risco tecnológico versus cibernético, mas também uma cadeia de riscos tecnológicos, sociais e económicos, originando perigos, fruto dos riscos existentes, bem como em outros territórios e espaços dentro ou fora do perímetro do TA, por diversas razões políticas, sociais, profissionais e financeiras.

Cibernética[1] é a capacidade de perceber a relação do Homem junto com outras teorias, áreas do saber; não é apenas de segurança, mas também de segurança entre Homem-Maquinaria, de como a informação pode ser assegurada. Mas também estuda o ser humano, procurando perceber até que ponto a evolução da tecnologia beneficia ao Homem e a sociedade no geral.

4 CARACTERIZAÇÃO DE TIPOS DE ATAQUES CIBERNÉTICOS

Os ataques cibernéticos são uma grande ameaça para o avanço da tecnologia, da comunicação, da atividade empresarial, da atividade estatal como um órgão que visa satisfazer as necessidades coletivas do povo dentro do seu território e com seu próprio sistema político, que se consubstancia na aplicação de princípios aceites a escala nacional e a nível internacional. E uma das estratégias encontradas pelos Estados é o desenho da descentralização de poderes (poder legislativo, executivo e judicial), neste contexto, a função judicial tem implantado serviços tecnológicos para fazer face a sua cadeia de valor. Porém, estes serviços encontram diversas ameaças versus tipos de riscos cibernéticos tais como:

[1] Caetano (2023). Aula doutoral do dia 06 de junho no Módulo Riscos Cibernéticos. Tema: Riscos Cibernéticos. Universidade Técnica de Moçambique (UDM). Faculdade de Ciências Económicas e Sociais.

Engenharia Social que consiste na manipulação psicológica que um criminoso prática contra uma pessoa para que ela realize ações ou lhe forneça dados confidenciais, incluindo informações pessoais, senhas ou credenciais eletrónicas. Em geral, faz isso por meio de e-mails que dão acesso a sites falsos, mensagens instantâneas com links maliciosos ou telefone com conteúdos que caracterizam situações de urgência ou oportunidades imperdíveis e com prazo curto para expirar[2].

A melhor forma de prevenção contra engenharia social é treinar e consciencializar a equipa com relação às principais ameaças aos dados dos mesmos e do negócio, para além de introduzir soluções de cibersegurança que protejam, detetem e combatam ações maliciosas no sistema.

Sistemas não corrigidos e configurações incorretas os quais ocorrem em ambientes digitais que se encontram desprotegidos em alguma de suas pontas porque suas configurações não foram feitas corretamente ou porque estão desatualizadas, ou seja, uma porta de entrada bastante eficiente para os cibercriminosos (Pacheco, 2019).

A melhor estratégia de solucionar ou reduzir este risco é melhorar a cibersegurança, investindo na monitoração ativa e automatizada das configurações e atualizações do ambiente digital, incluindo todas as soluções que o integram, contando com o apoio de parceiros de tecnologia de informação (TI) e sistema de informação (SI) especializados.

Ransomware ou *Phishing* que é um tipo de software malicioso (*malware*) que tem o poder de bloquear e criptografar informações e/ou ambiente, com promessa de reversão da situação apenas mediante o pagamento de resgate. Ele se instala no computador, no sistema da organização ou na rede corporativa após a permissão de um usuário vítima de um e-mail de *phishing* ou outro tipo de engenharia social. Também pode se instalar por meio de uma vulnerabilidade de sistemas carentes de correção ou atualização[3].

A estratégia de prevenir este maléfico tecnológico é ter uma rotina de backup robusta, eficiente e ininterrupta para, em caso de ataques, poder restabelecer o ambiente com menos prejuízos de informação e contar com soluções de segurança de *Endpoint* preparadas para esse tipo de ataque. É importante, também, contar com Serviços Gerenciados de TI tanto para mapear o funcionamento do ambiente quanto para mapear falhas e recuperar a funcionalidade diante de falhas e instabilidades. Periodicamente, aconselha-se a realização de rotinas de PenTest, que, por meio de tentativas de invasão de um hacking ético, identifica e testa vulnerabilidades.

Preenchimento de Credenciais que se caracteriza pelo uso de credenciais roubadas de colaboradores ou clientes de uma organização para acessar ambientes digitais de outras empresas. Trata-se de um ataque bastante popular e, muitas vezes, bem-sucedido, tendo em vista o grande número de listas de logins e senhas originais que são vendidas na *dark web* e do nocivo hábito das pessoas padronizarem login e senha. Essa ação pode ser executada por cibercriminosos ou robôs mal-intencionados (Ministério de Saúde Brasileiro, 2021).

Aqui, o desenho de uma boa prática de cibersegurança para reduzir ou eliminar este risco é essencial a eficiência da prática no múltiplo fator de autenticação, que pede para que o usuário confirme sua própria identidade mais de uma vez e implementar um programa de gestão de acessos privilegiados (PAM).

Ataques de Quebra de Senha por onde os criminosos utilizam uma solução de tecnologia capaz de, incansavelmente, testar uma série de possíveis combinações de caracteres para acessar ambientes digitais restritos a quem tem um login e uma senha legítimos. É sem dúvida, um desafio da cibersegurança (Martins, Lima & Bruschi, s/d).

Mais uma vez o fator humano é peça fundamental para dificultar a acção dos criminosos. A recomendação é orientar os colaboradores a criarem senhas que não tenham nenhuma relação com sua vida pessoal ou profissional. Além disso, é importante que sites e aplicações considerem em sua esteira de desenvolvimento um número máximo de tentativas de acesso, considerando a inserção de senhas incorretas.

[2] Proteja a sua pequena empresa sem esforço - Engenharia Social. Disponível: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering, indagado no dia 20 de Julho de 2023.

[3] Caetano (2023). Aula doutoral do dia 03 de julho no Módulo Riscos Cibernéticos. Tema: Riscos Cibernéticos_ Tipos de ataques. Universidade Técnica de Moçambique (UDM). Faculdade de Ciências Económicas e Sociais.

Man In the Middle (MitM) que consiste na ação do cibercriminosos de se posicionar entre um usuário e um aplicativo para intercetar os dados que estão sendo transacionados, em credenciais ou informações confidenciais e pessoais, sem prejudicar a experiência, ou seja, de maneira despercebida (de Andrade & dos Santos, 2018).

Neste tipo de crime tecnológico, aconselha-se a orientar aos colaboradores o uso da palavra-chave, incluindo evitar o uso de conexões wi-fi não seguras, gratuitas ou desprovidas de senhas, além de finalizar a sessão sempre que deixar um ambiente digital e verificar a cibersegurança do site antes de iniciar a navegação. É, ainda, uma boa prática oferecer uma Virtual Private Network aos colaboradores.

Ataques de Negação de Serviço conhecido pela sigla DoS, que é um acrónimo para Denial of Service, o Ataque de Negação de Serviço se caracteriza na ação do hacker de sobrecarregar um site com tráfego e dados para que ele se torne inacessível. Dependendo do perfil da página, esse ataque pode gerar a perda de vendas, além do investimento de tempo e recursos financeiros para restabelecer a funcionalidade do ambiente (Pessoa, 2015).

Para eliminar ou reduzir este risco é necessário é manter a atualização tanto do antivírus quanto dos patches de cibersegurança. Paralelamente a isso, monitore os relatórios de tráfego da página para detetar e investigar de maneira imediata e proactiva possíveis alterações de padrões.

Drive-by download que consiste na ação dos cibercriminosos de injetar *malwares* em sistemas de softwares ou *firewalls* desatualizados, apenas aproveitando vulnerabilidades dos ambientes, sem que seus usuários tenham executado nenhuma ação (Le, Welch, Gao & Komisarczuk, 2013).

A melhor prevenção é manter a atualização do sistema operacional, dos navegadores, dos aplicativos e dos softwares de cibersegurança. Diante das perspetivas desafiadoras para a adaptação a ambientes digitais cada vez mais complexos, principalmente considerando as nuances da infraestrutura de TI de cada organização, se manter atento às tendências é mandatário.

5 DESCRIÇÃO DA ÁREA DE ESTUDO

O TA é um órgão central e localiza-se na Cidade de Maputo, junto à Praça da Independência, n.º 1117, contactável pelo correio eletrónico: www.ta.gov.mz e ta@ta.gov.mz e de acordo com a Constituição da República de Moçambique-CRM (2018), o TA é o órgão superior da hierarquia dos tribunais provinciais, fiscais e aduaneiros. Este órgão é composto por pelo (a) Presidente do Tribunal e 18 Juízes Conselheiros (artigo 18 da Lei n.º 24/2013, de 1 de novembro, alterada e republicada pela Lei n.º 7/2015, de 6 de outubro). O artigo 229, CRM (2018) e a Lei n.º 24/2013, de 1 de Novembro, alterada e republicada pela Lei n.º 7/2015, de 6 de Outubro descrevem as reais competências e atribuições do TA que resumem-se em garantir a justiça Administrativa, Fiscal e Aduaneira ao cidadão, bem como o controlo da boa gestão e da utilização dos erários públicos, com uma visão de ser uma instituição célere e eficaz na promoção da integridade, legalidade e boa gestão da Administração Pública, com valores na persecução do cumprimento da sua missão, este órgão pauta a sua atividade por meio de: eficiência e eficácia, transparência, integridade, independência, relevância, conhecimento, proximidade e abertura.

6 DISCUSSÃO DOS RESULTADOS

O TA conta com 540 colaboradores agrupados em diversos serviços que respondem com eficácia as atribuições deste Órgão do estado. As atividades são desenvolvidas em um ambiente das Tecnologias de Informação e Comunicação bastante modernos onde cada colaborador tem acesso ao equipamento informático de mesa e algum portátil que varia de 7ª a 11ª geração com diferentes capacidades de processamento e armazenamento com modelos de referência probook e Elitebook todos usando o sistema operativo windows 10 com licenças do governo eletrónicas atualizadas por um ano renovável. Para a edição de documentos, elaboração de matrizes, tabelas entre outros de carácter administrativo, os computadores correm o Microsoft Office 2013, standard com licença

eletrónica do Governo atualizada assim como tem instalado o antivírus atualizado e licenciado por um exercício económico. Por conveniência, o navegador de internet peculiarmente em uso neste equipamento informático, tendo em conta que correm sistemas diversos de gestão, controlo, cadastro e produção de documentos e dados tais como ETA e MSEAT (para os serviços da Contadoria de Contas e Auditoria), VISTO (para os serviços de Contadoria do Visto), SGD (para os serviços de Gestão Documental), SGB (para os serviços do Gabinete da Biblioteca), BSC (para serviços da planificação), MARVEL-tis (para a Gestão Financeira), PONTO ELECTRÓNICO (para a Gestão de Recursos Humanos), SAP(Para a Administração e Finanças), SGCONTENCIOSOS (para todos os cartórios), EPROCURMENT (para serviços da UGEA), é o Google CHROME. Estes sistemas funcionam de forma padronizada, independente e não sincronizada devido ao conjunto, também diverso, dos serviços e dos objetivos por alcançar.

Este conjunto diversificado de sistemas de Informação e Comunicação em uso no TA está alojado em um datacenter composto por servidores locais com capacidade suficiente para o armazenamento de dados e um centro de recuperação de desastres onde toda a informação produzida é replicada para evitar danos à informação, perda ou furto. O Sistema de Servicedesk, faz o suporte técnico aos constrangimentos informáticos que os utilizadores possam eventualmente ter durante a operacionalização dos sistemas, e na base dos planos semanais e mensais pré-concebidos, são realizadas as manutenções de rotina a fim de garantir a atualização dos pacotes informáticos e ferramentas de acordo com a necessidade, limpeza dos SPYWARES e MALWARES que frequentemente atacam os sistemas operacionais deste órgão Administrativo do Estado.

Da caracterização funcional dos sistemas de Informação e Comunicação em uso no TA, é evidente a dispersão de um conjunto de sistemas padronizados para responder a diversos serviços delegados àquele órgão do Estado. Contudo, os mesmos embora padronizados mostram uma vulnerabilidade pela ausência da sincronização o que deixa de refletir um todo sistémico capaz de sofrer algum ataque cibernético. Dos dados obtidos, verifica-se uma disfunção quer por parte dos utilizadores dos equipamentos informáticos quer por parte dos colaboradores do servicedesk a medida em que se regista ataques cibernéticos recorrentes do tipo Drive-by download (*malwares* e spywares) enfatizados pelos autores Le, Welch, Gao & Komisarczuk (2013) como resultado de desatualizações dos sistemas operativos dos equipamentos. Levanta-se nesta discussão a hipótese do registo dos ataques deste tipo Drive-by download o facto do uso do Microsoft Office 2013 cuja aplicabilidade está desfasada da contemporaneidade. Isto é, os sistemas de Informação e Comunicação instalados dos equipamentos do TA obedecem a padrões de design contemporâneos que, em algum momento podem entrar em dissonância com o pacote da Microsoft 2013 cuja atualização está na versão 365 Apps. Portanto, o uso do Microsoft Office 2013 não oferece segurança suficiente no momento da atualização de algumas aplicações para a sua contínua funcionalidade. Daí que o Drive-by download encontra espaço para o seu ataque.

Para além deste ataque ser perpetrado pela desatualização dos sistemas ou aplicações, referencia-se o transporte do vírus, seja ele, do tipo Drive-by download ou não através dos discos duros portáteis vulgarmente conhecidos por Pen drive no âmbito de troca de documentos ou transporte dos mesmos de um computador portátil ao de mesa sem antes deixar correr o antivírus para a sua limpeza e garantia de segurança.

Em paralelo a estas vulnerabilidades, verifica-se o armazenamento de dados do TA em servidores locais. Embora haja um centro de recuperação de desastres, a margem da ocorrência do risco cibernético é maior na medida em que um servidor local é comummente caracterizado pela existência de infraestruturas físicas suscetíveis a degradação pelas mudanças climáticas, incêndios ou desmoronamentos.

7 MEDIDAS DE MITIGAÇÃO DO RISCO CIBERNÉTICO NO TRIBUNAL ADMINISTRATIVO

Um ataque cibernético bem-sucedido no TA causaria falhas nos diversos sistemas instalados ou mesmo interromperia as operações do TA, resultando em perda de produtividade pelo tempo de inatividade e consequentemente perda financeira com um impacto significativo no funcionamento

do estado, na reputação da organização e consequentemente uma diminuição da confiança para outros órgãos do estado e ao público em geral.

A prevenção dos riscos cibernéticos depende das peculiaridades de cada organização, e o primeiro passo é identificar e avaliar os riscos existentes para entender como elaborar uma estratégia de prevenção. No entanto, algumas práticas comuns de segurança cibernética são fortemente recomendadas para este tipo de riscos cibernéticos associados ao uso dos sistemas de informação e comunicação no TA tais como; investir em treinamento do pessoal colaborador afim de adotá-los de conhecimentos básicos de controlo dos planos de atualização das aplicações básicas, interpretar as notificações para a atualização, uso eficiente dos equipamentos, cumprimento dos calendários de manutenção, cumprimento das políticas internas do uso dos equipamentos e reportar as inconsistências registadas durante o trabalho; uso da nuvem para o armazenamento de dados em servidores remotos ao invés dos servidores locais para conferir maior proteção às informações em relação a ataques cibernéticos, além de permitir que o usuário acesse os dados de diferentes dispositivos conectados à Internet e massificar as monitorias constantes e contínuas por parte dos serviços de apoio (servicedesk) de modo a garantir o funcionamento pleno dos equipamentos, identificar riscos e adotar medidas de mitigação apropriadas.

Além disso, distintos órgãos do Estado possuem regulamentações específicas sobre proteção de dados e segurança cibernética do governo daí que, é primordial, ter uma estratégia adequada de mitigação de riscos que auxilia na conformidade com essas regulamentações, evitando penalidades legais e demais problemas, de modo a desviar os ataques no TA; elaborar e implementar planos de resposta a incidentes identificados tais como os treinamentos regulares dos colaboradores, armazenamento de dados na nuvem e monitoria contínua dos equipamentos.

Outrossim, é necessário no âmbito da programação orçamental do TA definir uma rubrica que zele pelas despesas locais de investigação e reparação de sistemas comprometidos, investir em programas de consciencialização contínuos sobre as ameaças cibernéticas, promovendo uma cultura de segurança e preparando as pessoas para reconhecer e responder adequadamente a possíveis ataques, para não colocar em causa a cadeia de valores da entidade.

8 REFERÊNCIAS

Amaro, J.J.V. (2005). Sociedades Complexas e Risco Ecológico – Epistemologia e Meio Ambiente na Actual Teoria De Sistemas. DOI: 10.5216/teri.v3i1.27324. Terceiro Incluído Issn 2237-079x Nupeat – Iesa-Ufg, V.3, N.1, Jan./Jun., 2013, P. 47 - 59, Artigo 37.

De Andrade, D. Q & dos Santos, G. C. S. (2018). Ataque de Homem do Meio em Aplicações de Realidade Virtual. Bacharelato em Tecnologia. Universidade Federal do Estado do Rio de Janeiro. Rio de Janeiro.

International Oganization of Standardization (ISO) (2009).Technical Management Board Working Group. Risk Manangement-Principles and Guidelines. Switzerland: International Oganization of Standardization.

Le, V. L; Welch, I; Gao, X & Komisarczuk, P. (2013). Anatomy of Drive-by Download Attack. Proceedings of the Eleventh Australasian Information Security Conference. Adelaide.

Lei n.º 1/2018, de 12 de Junho. Aprova a Constituição da Republica de Moçambique. Maputo. BR n.º 115. I Série, 2º suplemento. Imprensa Nacional de Moçambique, EP.

Lei n.º 7/2015, de 6 de Outubro. Aprova a Lei de Orgânica da jurisdição Administrativa. Maputo. BR n.º 79. I Série. Suplemento. Imprensa Nacional de Moçambique, EP.

Lima, J.R.A & da Silva, J.G. (2012). Tecnologia: Conceitos e percepções discentes de nível Tecnológico. Congresso Norte Nordeste de Pesquisa e Inovação. Brasil.

Martins, A. L Lima; Lima, E. F & Bruschi, G. (s/d). Segurança em Banco de Dados: Teste de Quebra de Senha por Força Bruta no Banco de Dados Oracle 11G. Curso de Tecnologia em Banco de Dados - Faculdade de Tecnologia de Bauru (FATEC). São Paulo.

Maluf, G. de B. (2023). Riscos cibernéticos: a importância de ter uma estratégia de mitigação. UPlexis Tecnologia. 6 de Junho. Disponível em https://uplexis.com.br/blog/artigos/riscos-ciberneticos. Indagado no dia 20 de Julho de 2023.

Ministério de Saúde Brasileiro. (2021). Departamento de Informática do SUS. Manual de Apoio para Solicitações de Credenciais no Portal de serviços. Brasília.

Pacheco, F. G. (2019). Análise das Técnicas de Segurança do Framework Laravel Contra Ataques as Aplicações Web. Bacharelato em Ciências de Computação. Universidade Federal Rural De Pernambuco. Garanhuns.

Pessoa, J. (2015). Estratégia para tratamento de ataques de negação de serviço na camada de aplicação em redes IP. Mestrado em Informática. Universidade federal de Paraíba.

Resolução n.º 69/2021, de 31 de Dezembro. Aprova a Política de Segurança Cibernética e Estratégia da sua Implementação. Maputo. BR n.º 253. I Série, 12º suplemento. Imprensa Nacional de Moçambique, EP.

Santos, S.I. da Silva. (2015). A Acção do Estado em Matéria de Cibersegurança. Trabalho de Seminário de Investigação em Administração Pública. Universidade de Lisboa: Instituto Superior de Ciências Sociais e Políticas. Lisboa.