Análise de Vulnerabilidades dos Portais Web das Câmaras Municipais Alagoanas

Eduardo V. Vieira Torres[1], **Daniel Fireman (orientador)** [1]

[1]Bacharelado em Sistemas de Informação – Instituto Federal de Alagoas (IFAL) – Arapiraca – AL – Brasil

evvt1@aluno.ifal.edu.br, daniel.fireman@ifal.edu.br

Abstract. *With the rise of internet access in Brazil, government web portals fulfill an essential role. With that increase in usage, public online information systems have become a target of cybercriminal attacks. This work analyzed the 102 Alagoas city council web portals searching for vulnerabilities according to The Open Web Application Security Project (OWASP) Top 10 classification of 2021. The results revealed a total of 667 vulnerabilities, with* 10% *critical. Furthermore, we tried to explain these vulnerabilities by finding correlations with the city Gross Domestic Product (GDP) and the usage of the open-source Interlegis portal. Finally, we provide actionable advice on improving the security of those information systems, which are essential to Brazilian democracy.*

Resumo. *Com a popularização do acesso a internet no Brasil, portais eletrônicos governamentais cumprem um papel essencial. Com esse crescimento na utilização, sistemas de informação públicos se tornaram um alvo de ataques de criminosos cibernéticos. Este trabalho analisou os portais eletrônicos das 102 câmaras municipais alagoanas de acordo com a classificação The Open Web Application Security Project (OWASP) Top 10 de 2021. Além disso, explicamos essas vulnerabilidades através de correlações com o produto interno bruto e o uso do portal de código aberto Interlegis. Por fim, sugerimos medidas práticas de como melhorar a segurança destes sistemas de informação, os quais são essenciais para a democracia brasileira.*

1. Introdução

Instituições públicas e privadas vem adotando as mais variadas soluções tecnológicas baseadas na web para aprimorar seus processos e facilitar a execução de suas atividades-fim. Concomitantemente a isso, pessoas mal-intencionadas surgem cometendo crimes cibernéticos visando o roubo de informações ou o comprometimento da usabilidade, como relata o trabalho de [Wendt and Jorge 2013].

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) revela que durante o ano de 2020 aconteceram 1.822 ataques por dia [CERT.BR 2020]. Tais dados demonstram o quão rotineiros são os ataques *hackers* contra instituições públicas e privadas, os quais podem afetar tanto a confidencialidade dos usuários, quanto as operações dessas instituições. Nesse sentido, [Agra and Barboza 2019] definem vulnerabilidade como uma brecha que atacantes podem utilizar para burlar o funcionamento correto de um sistema, ou ainda, roubar informações do mesmo.

Vulnerabilidades de segurança são pontos fracos de um sistema. No entanto, a falta de educação das pessoas em segurança da informação pode gerar problemas. Conforme [Mitnick and Simon 2003], as pessoas podem ser consideradas os elos mais fracos da segurança de um sistema, ou seja, cibercrimonosos podem enganar pessoas a fim de roubar informações confidenciais. Desse modo, como exemplo, no âmbito empresarial, segundo [Hayden 2015], as organizações carecem de uma cultura de mentalidade de segurança que seja capaz de fornecer hábitos, comportamentos e normas que estejam alinhados à segurança da informação aos seus colaboradores.

Por outro lado, sob a perspectiva de sistemas de informação, o estado de Alagoas possui um total de 102 municípios com mais de mil vereadores em atividade nas câmaras municipais. Os portais eletrônicos das câmaras são sistemas de informação que disponibilizam informações sobre o exercício legislativo e permitem a interação cidadã. Um módulo de destaque destes portais é o de transparência, que publiciza informações acerca da execução orçamentária e financeira (receitas e despesas), dentre outras informações de interesse do cidadão. Outro componente importante é o sistema eletrônico de informações ao cidadão (e-SIC), que permite a realização de pedidos de acesso à informação.

O governo federal disponibiliza um modelo de portal gratuito e de código-fonte aberto chamado de Portal Modelo Interlegis ou Modelo Interlegis [Senado Federal 2023]. Ele vem pronto para ser usado pelas câmaras municipais e foi concebido com foco em usabilidade, acessibilidade e segurança. Devido a essas vantagens e as restrições orçamentárias, seria esperado uma adoção massiva entre as câmaras municipais.

Atualmente, não há informações sobre vulnerabilidades de segurança em portais eletrônicos das câmaras municipais alagoanas, seja ele do tipo Interlegis ou não. Dada a importância e o uso destes sistemas de informação, é imperativo conhecer e corrigir suas vulnerabilidades, impossibilitando que atacantes roubem ou modifiquem informações sobre, ou para os cidadãos. Ademais, a integridade das informações das câmaras são de extrema importância para garantir que a Lei de Acesso à Informação (LAI) esteja sendo cumprida pelo município. Se houver vulnerabilidades de segurança nesses portais, atacantes podem adulterar informações anteriormente íntegras e fazer com que a LAI seja descumprida, prejudicando o acesso a informações legítimas por parte dos cidadãos neste tipo de site.

O presente trabalho tem como objetivo geral verificar eventuais vulnerabilidades de segurança existentes em portais das câmaras municipais do estado de Alagoas. Têm-se como objetivos específicos:

1. Analisar vulnerabilidades dos portais eletrônicos conforme a classificação *Open Web Application Security Project* (OWASP) de criticidade. Além da análise geral, escolhemos dois focos específicos:
    - Portais de câmara que utilizam o Portal Modelo Interlegis do Governo Federal;
    - Relação entre as vunerabilidades encontradas e os orçamentos das câmaras, usando o Produto Interno Bruto (PIB) como medida indireta;
2. Discutir possíveis soluções e medidas de prevenção para as vulnerabilidades encontradas.

Como algumas contribuições desse estudo, tem-se que não foram encontradas vulnerabilidades em 9, dos 100 portais analisados. O total de vulnerabilidades detectadas foi

667 ($\approx 7,3$ em média). Ademais, os resultados nos indicam que o orçamento das câmaras legislativas não é proporcional às medidas de segurança dos portais eletrônicos. Já os portais baseados no Portal Modelo Interlegis não possuem vulnerabilidades críticas.

Sobre a organização das demais seções deste trabalho tem-se: a Seção 2 evidencia a fundamentação teórica e na Seção 3 são introduzidos trabalhos relacionados a este estudo. Apresentamos a metodologia na Seção 4. Em seguida, na Seção 5 são apresentadas as análises de vulnerabilidades e na Seção 6 sugestões práticas para correção das vulnerabilidades encontradas. Por fim, as considerações finais e trabalhos futuros são apresentados na Seção 7.

2. Fundamentação Teórica

2.1. Segurança da Informação

Segurança da informação é definida por meio da ISO 27000 como sendo a preservação da confidencialidade, integridade e disponibilidade das informações. Adicionalmente, outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas [ISO 2018]. As características a serem preservadas podem ser definidas como:

- Confidencialidade: manter restrições sobre a divulgação e acesso de informações, com a finalidade de conservar a privacidade de informações e indivíduos. Se, por exemplo, um banco de dados não tiver uma política de controle de acesso para usuários, então os dados cadastrados podem ser vazados, gerando uma quebra de confidencialidade.
- Integridade: manter informação buscando preservá-la contra modificações ou destruição imprópria incluindo a irretratabilidade e autenticidade. Suponha que um servidor seja invadido e dados tenham sido alterados sem se ter tenha mecanismos de backup, nesse caso a integridade das informações foi comprometida.
- Disponibilidade: garantir o acesso rápido e confiável a informação. Um ataque pode ser realizado contra algum site com o objetivo de torná-lo indisponível. Caso isso aconteça e o ataque seja bem-sucedido, a disponibilidade estará comprometida.

2.2. Vulnerabilidades

Segundo [Martinelo and Bellezi 2014], uma vulnerabilidade pode ser definida como um ponto falho em um sistema que permita a realização e a concretização de um ataque a um sistema computacional.

Dentre as vulnerabilidades existentes, há as que afetam sistemas web. Essas são estudadas e listadas por [OWASP 2021], sendo organizadas em uma lista com as dez vulnerabilidades mais críticas (OWASP Top 10). A OWASP ou *The Open Web Application Security Project* é uma fundação que tem como objetivo melhorar a segurança de softwares permitindo que indivíduos ou empresas tomem decisões embasadas. A classificação da OWASP consiste nos seguintes grupos:

1. (A1) Quebra de Controle de Acesso;
2. (A2) Falhas Criptográficas;
3. (A3) Injeção;

4. (A4) Design Inseguro;
5. (A5) Configuração Incorreta de Segurança;
6. (A6) Componentes Vulneráveis e Desatualizados;
7. (A7) Falhas de Autenticação e Identificação;
8. (A8) Falhas de integridade de software e dados;
9. (A9) Falhas de Monitoramento e Logs de segurança;
10. (A10) Falsificação de requisições para o lado servidor (SSRF).

3. Trabalhos relacionados

Inicialmente, [Reis et al. 2018] foca em analisar vulnerabilidades do sistema de *Internet Banking* de 20 instituições financeiras (IFs) tentando entender se há relação entre o patrimônio líquido de uma IF com um número maior ou menor de vulnerabilidades. As ferramentas usadas no estudo foram os *scanners* [VEGA 2023] e [SKIPFISH 2023]. O número de vulnerabilidades total encontrado por [Reis et al. 2018] foi de 1.938, as quais pertencem a oito categorias de vulnerabilidade segundo a [OWASP 2017]. As vulnerabilidades que obtiveram maior frequência foram: Configuração Incorreta de Segurança (626), Entidades Externas XML (568) e Injeção (290).

O estudo de [Reis et al. 2018] negou a hipótese inicial e concluiu que nenhum indicativo mostrou que exista uma forte correlação entre o patrimônio líquido de uma IF e a segurança de seu portal de *Internet Banking*, porém foi possível encontrar uma correlação entre o número de acessos de uma IF e a alta criticidade das vulnerabilidades encontradas nos respectivos sistemas.

De forma análoga ao trabalho de [Reis et al. 2018], [Sena et al. 2017] usa uma abordagem que recorre a um único *scanner*, o [NETSPARKER 2023], e os sites analisados compõem um total de 40 portais de prefeituras do Estado da Paraíba. O trabalho classificou as vulnerabilidades conforme a [OWASP 2017]. Os resultados encontrados no estudo revelaram um total de 822 vulnerabilidades de 12 tipos diferentes, com relação à frequência entre as vulnerabilidades de maior criticidade têm-se: *Cross-site Scripting* (52%) e *Out of Date Version (*26%*)*. Conforme [Sena et al. 2017], 30% do total de vulnerabilidades são críticas e de alta criticidade, o que indica fragilidade, por parte da Administração Pública, no gerenciamento e controle da segurança da informação dos portais analisados.

Semelhantemente ao trabalho de [Sena et al. 2017], o estudo de [Costa et al. 2017] analisa a segurança dos portais de governos eletrônicos dos 26 estados, do distrito federal e do governo federal sob a perspectiva do número de vulnerabilidades encontrado em cada portal e verifica a hipótese referente a uma possível relação do poderio econômico dos estados donos dos portais com o número de vulnerabilidades encontrado. A abordagem usada por [Costa et al. 2017] utiliza dois *scanners* de vulnerabilidades, o [SKIPFISH 2023] e o [UNISCAN 2023]. Em adição, o estudo utiliza o [NMAP 2023] para varredura de portas abertas nos portais analisados.

O trabalho de [Costa et al. 2017] revelou 5.193 vulnerabilidades de três tipos da [OWASP 2017]: Redirecionamento e Encaminhamentos Inválidos (97%), Cross-site Scripting ($2,5\%$) e Injeção ($0,5\%$). O estudo teve como conclusão o fato da hipótese ter sido negada, e, dessa forma, estados mais ricos obtiveram um número maior de vulnerabilidades comparado com os mais pobres.

Os estudos mencionados acima respaldaram a metodologia deste trabalho e auxiliaram a estruturar uma análise de vulnerabilidades de portais de governos eletrônicos. Apesar de possuir semelhanças, como, por exemplo, usar apenas um *scanner* de vulnerabilidades e não verificar portas abertas nos portais, este estudo é o primeiro a analisar vulnerabilidades dos portais de todas as câmaras legislativas dos municípios de Alagoas. Por fim, este trabalho inicia a busca por relações que expliquem tais vulnerabilidades e propõem soluções para melhorar o estado da prática.

4. Metodologia

Para realizar a análise de vulnerabilidades, foram levantadas as URLs e as empresas/instituições desenvolvedoras dos portais. Dado que os municípios de São Brás e Traipu não possuem um portal dedicado a câmara legislativa municipal, não serão avaliados neste estudo. A metodologia utilizada nesse trabalho é ilustrada no diagrama da Figura 1.

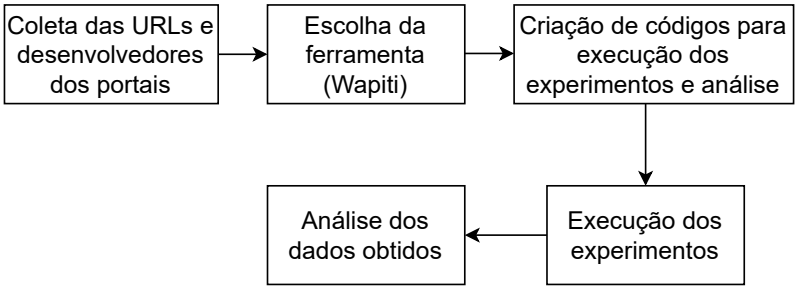

Figura 1. Diagrama exibindo a metodologia utilizada. Produzido pelo autor.

A ferramenta de scanner de vulnerabilidades usada neste estudo foi o [WAPITI 2023] na versão 3.1.4. Tal ferramenta foi escolhida por ser gratuita, de código aberto e de fácil uso. Por fim, possui uma boa popularidade no meio acadêmico (823 artigos mencionam a ferramenta no Google Scholar) e possibilita exportar o relatório de vulnerabilidades em diversos formatos diferentes como HTML, JSON e XML [Google 2023].

O experimento realizado para obtenção dos dados das vulnerabilidades para análise estatística posterior possui as vulnerabilidades como variáveis dependentes e as URLs dos portais das câmaras como único fator, com 100 possíveis níveis. As constantes do experimento são a ferramenta utilizada, uso dos módulos de ataque padrão, o ambiente experimental e os parâmetros da ferramenta: tempo máximo de *scan* em 720 segundos e tempo máximo de execução de cada módulo em 648 segundos.

O ambiente experimental utilizado é composto de 100 máquinas virtuais do tipo t2.micro do serviço EC2 da [AWS 2023]. Máquinas virtuais do tipo t2.micro possuem armazenamento EBS, 1 GB de memória RAM e 1 vCPU. O número de máquinas virtuais é igual ao número de tratamentos experimentais. As análises, com objetivo de produzir os relatórios de vulnerabilidade de cada URL, foram divididas em quatro etapas: as primeiras três etapas analisaram 30 URLs e a última 10 URLs.

Para automatizar a execução dessas etapas foram usadas as tecnologias [TERRAFORM 2023] e [ANSIBLE 2023], caracterizadas como ferramentas de Infraestrutura como código (IAC). O [TERRAFORM 2023] foi usado para obter e iniciar a

quantidade de máquinas virtuais necessárias para a execução dos experimentos na AWS. Já o [ANSIBLE 2023] foi utilizado para automatizar a instalação da ferramenta de análise e a execução dos experimentos nas máquinas previamente iniciadas[1].

5. Resultados da Análise de Vulnerabilidades

Iniciamos ressaltando que em 9 portais não foi detectado nenhum tipo de vulnerabilidade. São eles os portais das câmaras de Arapiraca, Cacimbinhas, Chã Preta, Feliz Deserto, Jacaré dos Homens, Messias, Palestina, Piranhas e Teotônio Vilela.

O total de vulnerabilidades encontradas, considerando todos os portais, foi de 667. Dentre os portais das câmaras legislativas que foram encontradas vulnerabilidades, os municípios de Maragogi e Penedo se destacaram com 26 vulnerabilidades, o maior número. No extremo oposto, com apenas uma vulnerabilidade detectada, temos Belém, Belo Monte, Cajueiro, Carneiros, Colônia Leopoldina, Girau do Ponciano, Maribondo, Satuba e Senador Rui Palmeira.

Os tipos de vulnerabilidades identificadas foram: Quebra do Controle de Acesso (A1), Injeção (A3), Design Inseguro (A4) e Configuração Incorreta de Segurança (A5). A Tabela 1 ilustra a distribuição das vulnerabilidades descobertas conforme a classificação da [OWASP 2021]. Proporcionalmente, as vulnerabilidades são de: Configuração Incorreta de Segurança com $52,5\%$, seguido de Design Inseguro com $45,12\%$ e por fim, Injeção com $2,25\%$ e Quebra do Controle de Acesso com $0,13\%$.

Tabela 1. Vulnerabilidades de acordo com a classificação da [OWASP 2021]

Vulnerabilidades	Frequência
A1	1
A3	15
A4	301
A5	350

Dez portais de câmaras ou 10% de todos os portais analisados apresentaram vulnerabilidades críticas, que são, neste estudo, as três primeiras classificações da [OWASP 2021]. São eles: Água Branca, Atalaia, Boca da Mata, Cajueiro, Delmiro Gouveia, Estrela de Alagoas, Porto Real do Colégio, Roteiro, Santana do Mundaú e Viçosa. As vulnerabilidades presentes nesses portais são, segundo a classificação [OWASP 2021], de duas categorias: A3 Injeção e A1 Quebra do Controle de Acesso.

5.1. Avaliação de vulnerabilidades em portais conforme o PIB das cidades

Um fator importante na construção de um sistema de informação é seu orçamento. Neste trabalho utilizamos o Produto Interno Bruto (PIB) das cidades como indicador do orçamento da câmara, que por sua vez, indica o montante disponível para os portais. A Tabela 2 mostra parâmetros estatísticos da distribuição de vulnerabilidades comparando os portais na lista das 10 cidades com maior PIB de Alagoas, de acordo com [WIKIPEDIA 2023], e os demais portais nos quais foram obtidas vulnerabilidades (total de 81).

[1]O código-fonte pode ser acessado em https://github.com/eduardovitor/ScriptsTCC

Tabela 2. Vulnerabilidades quanto ao PIB das cidades

	Maiores PIB (10)	Demais (81)
Média	11	7
Máximo	26	26
Desvio padrão	$9,23$	$6,5$

Estes resultados nos indicam que o orçamento das câmaras legislativas não é proporcional às medidas de segurança dos portais eletrônicos. A partir dos dados expostos, nota-se que as 10 cidades com maior PIB têm portais com número médio de vulnerabilidades de 11, número $1,6\times$ maior do que o restante dos portais de cidade.

Analisando a importância das vulnerabilidades detectadas, dentre as cidades com maior PIB, apenas portal de Delmiro Gouveia apresentou vulnerabilidades críticas (4). Já com relação aos demais portais, cerca de 10% deles apresentaram alguma vulnerabilidade de segurança crítica.

5.2. Avaliação de vulnerabilidades em portais do tipo Interlegis

O governo federal disponibiliza um modelo de portal gratuito para uso das Câmaras Municipais e Assembleias Legislativas chamado de Portal Modelo Interlegis que, conforme o site do senado federal, possui os padrões web exigidos para portais públicos: usabilidade, acessibilidade e segurança. O padrão web que este trabalho avalia é a segurança, buscando entender se, de fato, há um bom nível de segurança nesse tipo de site em termos de número de vulnerabilidades.

Nesse sentido, os portais de câmara que utilizam esse modelo são: Fleixeiras, Japaratinga, Jaramataia, Junqueiro, Marechal Deodoro, Murici, Olho D'água Das Flores, Paripueira, Pilar e Santa Luzia do Norte. Foram detectadas em média 12 vulnerabilidades não-críticas dos tipos: Design Inseguro (80%) e Configuração Incorreta de Segurança (20%).

A fim de avaliar vulnerabilidades em portais interlegis $(10$ portais) e não-interlegis $(81$ portais) foi utilizado um teste de hipótese não-paramétrico que verifica se dois conjuntos de dados independentes têm distribuições diferentes (*Mann Whitney U*). A hipótese nula foi que o número de vulnerabilidades em portais interlegis é igual ou menor do que o de portais não-interlegis. A hipótese alternativa foi que o número de vulnerabilidades em portais interlegis é maior do que o de portais não-interlegis.

Portais interlegis apresentaram uma média de 12 vulnerabilidades, com o máximo chegando a 19 e desvio-padrão de $5,73$. Já portais não-interlegis obtiveram uma média de 7 vulnerabilidades, com o máximo chegando a 26 e desvio-padrão $6,89$. O teste de hipótese realizado com nível de confiança de 95% apresentou um p-valor $0,001$. Este resultado indica, com alta confiança estatística, que devemos rejeitar a hipótese nula, isto é, o número de vulnerabilidades mediano em portais interlegis é maior do que o de portais não-interlegis.

Em contrapartida, nenhum portal que usa o modelo Interlegis apresentou vulnerabilidades críticas de segurança. Já com relação aos demais portais que não usam Interlegis, cerca de 11% deles apresentaram alguma vulnerabilidade de segurança crítica.

6. Sugestões Práticas para Correção das Vulnerabilidades Encontradas

6.1. Configuração Incorreta de Segurança

A vulnerabilidade "Configuração Incorreta de Segurança", que possui a quinta posição da classificação da [OWASP 2021] foi a mais frequente, com 350 ocorrências, ela foi encontrada em 81% dos portais de câmara analisados. A fim de eliminar as vulnerabilidades deste tipo é preciso verificar, revisar e atualizar as configurações de segurança em todo os sites. Além disso, é necessário atentar-se para usar uma arquitetura de software segmentada e o mínimo de bibliotecas e *framewoks*, evitando softwares desatualizados e por consequência componentes vulneráveis a ataques.

6.2. Design Inseguro

Sobre o segundo tipo de vulnerabilidade mais frequente "Design Inseguro", ela possui a quarta posição da [OWASP 2021] com 301 ocorrências sendo encontrada em 44% dos portais de câmara analisados. Como forma de prevenção e remediação deste tipo de vulnerabilidade, é aconselhável implementar um ciclo de desenvolvimento seguro de aplicações, usar bibliotecas de padrões de design seguro, limitar o consumo de recursos por usuário ou serviço. Além de tratar erros do site adequadamente para não incorrerem em liberação de informações sensíveis sobre os servidores onde o site está rodando.

6.3. Injeção

A terceira vulnerabilidade mais numerosa foi "Injeção", que possui a terceira posição da classificação da [OWASP 2021], com 15 ocorrências, ela foi encontrada em 10% dos portais de câmara analisados. Para evitar e corrigir vulnerabilidades deste tipo é preferível que se use uma API segura que não utilize o interpretador do banco de dados diretamente e impossibilite a execução de scripts maliciosos. Ademais, usar sanitização, filtro ou validação no lado do servidor é crucial para eliminar vulnerabilidades deste tipo. Nesse sentido, é importante escapar caracteres especiais de consultas e usar controles do SQL.

6.4. Quebra do Controle de Acesso

O tipo de vulnerabilidade menos frequente foi "Quebra de Controle de Acesso", que possui a primeira posição da classificação da [OWASP 2021], com apenas uma detecção. Para extinguir uma vulnerabilidade deste tipo, faz-se fundamental tomar algumas medidas como: negar acesso a quaisquer recursos não públicos no site como metadados e arquivos de backup, logar falhas de controle de acesso e desabilitar listagem de diretórios. Finalmente, limitar o número de requisições ao site em um mesmo período evita ataques por meio de ferramentas automatizadas.

7. Conclusão

De início, o presente trabalho alcançou seu objetivo com êxito ao verificar a existência de possíveis vulnerabilidades de segurança nos portais das câmaras municipais alagoanas. Além disso, este estudo descreveu e classificou as vulnerabilidades encontradas conforme a [OWASP 2021] e expôs a proporção de portais de câmara com vulnerabilidades críticas e não críticas.

O número total de vulnerabilidades encontrado foi de 667, com relação à proporção de vulnerabilidades críticas: 81% dos portais apresentaram vulnerabilidades

não críticas, 10% apresentaram vulnerabilidades críticas e 9% não apresentaram vulnerabilidades. As vulnerabilidades encontradas foram dos tipos: Quebra do Controle de Acesso (A1) com 0,13%, Injeção (A3) com 2,25%, Design Inseguro (A4) com 45,12% e Configuração Incorreta de Segurança (A5) com 52,5%.

Em seguida, este trabalho avaliou vulnerabilidades nos portais sob a perspectiva das 10 cidades alagoanas com maior PIB. Os resultados nos indicam que o orçamento das câmaras legislativas não é proporcional às medidas de segurança dos portais eletrônicos, dado que os portais das cidades com maior PIB apresentaram um número médio de vulnerabilidades maior do que as outras câmaras. Contudo, apenas o portal de Delmiro Gouveia apresentou vulnerabilidades críticas (4).

Finalmente, este trabalho avaliou vulnerabilidades de portais de câmaras que utilizam o Portal Modelo Interlegis em comparação aos que não utilizam e concluiu que câmaras que usam o modelo obtiveram um número médio de vulnerabilidades maior $(1,7x)$ do que câmaras que não usam. Todavia, não foram encontradas vulnerabilidades de segurança críticas em portais que usam o modelo. O número de vulnerabilidades não-críticas médio em portais Interlegis foi de 12 e os tipos encontrados foram Design Inseguro (80%) e Configuração Incorreta de Segurança (20%).

Como trabalhos futuros, pode-se verificar a existência de possíveis vulnerabilidades nos sites das prefeituras dos municípios alagoanos ou verificar a existência de vulnerabilidades em câmaras municipais de outro estado. Uma nova perspectiva de análise pode ser adotada considerando o uso de mais de uma ferramenta a fim de obter uma maior confiabilidade dos resultados obtidos. Finalmente, pode-se verificar a percepção dos usuários dos sistemas analisados quanto às vulnerabilidades detectadas.

8. Agradecimentos

Agradecemos a revisão minuciosa deste artigo e do TCC pelo professor Felipe Alencar Lopes. Finalmente, agradecemos também ao professor Matheus Torquato por sua revisão e sugestões de melhoria do TCC.

Referências

Agra, A. D. and Barboza, F. F. M. (2019). *Segurança de sistemas da informação*. Grupo A.

ANSIBLE (2023). Ansible. Disponível em: `https://www.ansible.com/`.

AWS (2023). Amazon ec2. Disponível em: `https://aws.amazon.com/pt/ec2/`.

CERT.BR (2020). Estatísticas do cert.br - incidentes. Disponível em: `https://www.cert.br/stats/incidentes/`.

Costa, J. V. P. et al. (2017). Análise de vulnerabilidades de segurança em portais de governos eletrônicos.

Google (2023). Google scholar. Disponível em: `https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0\%2C5&q=wapiti+vulnerability+scanner&btnG=`.

Hayden, L. (2015). *People-centric security: transforming your enterprise security culture*. McGraw Hill Professional.

ISO (2018). Iso iec 27000: Information technology — security techniques — information security management systems — overview and vocabular fifth edition.

Martinelo, C. A. G. and Bellezi, M. A. (2014). Análise de vulnerabilidades com openvas e nessus. *Revista TIS*, 3(1).

Mitnick, K. D. and Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

NETSPARKER (2023). Netsparker – web application security scanner. Disponível em: `https://www.100security.com.br/netsparker`.

NMAP (2023). The network mapper. Disponível em: `https://github.com/nmap/nmap`.

OWASP (2017). Owasp top 10 - 2017. Disponível em: `https://owasp.org/www-project-top-ten/2017/Top_10`.

OWASP (2021). Owasp top 10 - 2021. Disponível em: `https://owasp.org/Top10/`.

Reis, A. P. d. et al. (2018). Análise de vulnerabilidades de segurança em sistemas de internet banking utilizando ferramentas de código aberto.

Sena, A. S. d. et al. (2017). Portais de governo eletrônico em municípios do estado da paraíba: análise sob a óptica da segurança da informação.

Senado Federal (2023). Portal modelo - interlegis. Disponível em: `https://www.interlegis.leg.br/produtos-servicos/portal-modelo/`.

SKIPFISH (2023). Skipfish web application security scanner. Disponível em: `https://gitlab.com/kalilinux/packages/skipfish`.

TERRAFORM (2023). Terraform. Disponível em: `https://www.terraform.io/`.

UNISCAN (2023). Uniscan web vulnerability scanner. Disponível em: `https://www.kali.org/tools/uniscan/`.

VEGA (2023). Vega vulnerability scanner. Disponível em: `https://subgraph.com/vega/`.

WAPITI (2023). Wapiti - web vulnerability scanner. Disponível em: `https://github.com/wapiti-scanner/wapiti`.

Wendt, E. and Jorge, H. V. N. (2013). *Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação*. Brasport.

WIKIPEDIA (2023). Lista de municípios de alagoas por pib. Disponível em: `https://pt.wikipedia.org/wiki/Lista_de_munic\%C3\%ADpios_de_Alagoas_por_PIB`.