UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS – CENTRO DE EDUCAÇÃO
MESTRADO PROFISSIONAL EM GESTÃO EM ORGANIZAÇÕES APRENDENTES

Alnio Suamy de Sena

PORTAIS DE GOVERNO ELETRÔNICO EM MUNICÍPIOS DO ESTADO DA PARAÍBA: análise sob a óptica da segurança da informação

João Pessoa
2017

ALNIO SUAMY DE SENA

PORTAIS DE GOVERNO ELETRÔNICO EM MUNICÍPIOS DO ESTADO DA PARAÍBA: análise sob a óptica da segurança da informação

Dissertação apresentada ao Programa de Pós-Graduação em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito final para obtenção do Título de Mestre.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

Linha de Pesquisa: Gestão de Projetos Educativos e Tecnologias Emergentes

João Pessoa

2017

Catalogação na publicação
Universidade Federal da Paraíba
Seção de Processos Técnicos da Biblioteca Setorial do CCEN/UFPB

S474 p Sena, Alnio Suamy de.
Portais de governo eletrônico em municípios do estado da Paraíba : análise sob a óptica da segurança da informação / Alnio Suamy de Sena. – João Pessoa, 2017.
118 p. : il. color.

Dissertação (Mestrado Profissional em Gestão nas Organizações Aprendentes) – Universidade Federal da Paraíba.
Orientador: Profº Dr. Wagner Junqueira de Araújo.

1. Gestão da segurança da informação. 2. Governo Eletrônico. 3. *Scanner* de vulnerabilidades. I. Título.

BS/CCEN/UFPB CDU 004(043)

ALNIO SUAMY DE SENA

PORTAIS DE GOVERNO ELETRÔNICO EM MUNICÍPIOS DO ESTADO DA PARAÍBA: análise sob a óptica da segurança da informação

Dissertação apresentada ao Programa de Pós-Graduação em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito final para obtenção do Título de Mestre.

Aprovada em: 02 / agosto / 2017

BANCA EXAMINADORA

Professor Dr. Wagner Junqueira de Araújo /UFPB
Orientador (presidente)

Professor Dr. Marckson Roberto Ferreira de Sousa /UFPB
Examinador (interno)

Professora Dra. Alzira Karla Araújo da Silva / UFPB
Examinadora (externo)

AGRADECIMENTOS

Agradeço à minha mãe, que com seu exemplo, me educou e me preparou para os desafios da vida, mostrando que com perseverança e honestidade é possível fazer com que sonhos se tornem realidade.

Meus sinceros agradecimentos e profunda gratidão ao meu orientador Professor Dr. Wagner Junqueira de Araújo. Seu conhecimento, comentários construtivos e modo de pensar lógico me foram de grande ajuda. Agradeço também pelos ensinamentos e, principalmente, paciência dedicada para o bom andamento dessa pesquisa.

Agradeço aos Professores Dr. Marckson Roberto Ferreira de Sousa e Dra. Alzira Karla Araújo da Silva, por aceitarem participar da banca, o que com certeza, com suas críticas e sugestões, contribuíram para a melhoria dessa pesquisa.

Agradeço também aos amigos da turma 6 do mestrado de Gestão nas Organizações Aprendentes por se mostrarem sempre solícitos, em especial ao Fernando Souza que em muitos momentos me ajudou tanto em minha pesquisa quanto com palavras de incentivo.

RESUMO

O governo eletrônico pode ser caracterizado como a utilização das Tecnologias de Informação e Comunicação, pela administração pública, como apoio aos processos internos do governo e a entrega de produtos e serviços governamentais aos cidadãos e à indústria de forma célere e eficiente. É fundamental que o governo eletrônico se previna de acessos indevidos a fim de garantir que a Integridade, a Disponibilidade e a Confidencialidade, princípios basilares da segurança da informação, sejam protegidas de ameaças eletrônicas presentes na Internet. Essas ameaças colocam os ativos de informação em constante risco ao se aproveitarem das diversas vulnerabilidades existentes no ambiente virtual onde está inserido o governo eletrônico. Dessa forma, essa pesquisa analisa as possíveis vulnerabilidades existentes em portais de governo eletrônico em municípios do Estado da Paraíba. A população da pesquisa foram os 50 municípios que representam maior participação para a composição do Produto Interno Bruto (PIB) do Estado da Paraíba, sendo possível analisar os portais de 40 municípios. Esta pesquisa caracterizou-se como uma pesquisa descritiva, com abordagem quantitativa. Para a coleta dos dados utilizou-se o software Nestparker, um *scanner* de vulnerabilidades que tem como função rastrear e identificar vulnerabilidades em aplicações *Web*. Como resultado, foram encontradas 822 vulnerabilidades, das quais 15% são Críticas e 15% de Alta Criticidade. Além disso, 10% das vulnerabilidades foram classificadas como de Média Criticidade, o que, somada às outras vulnerabilidades de maiores impactos, representa um cenário com mais de 40% de vulnerabilidades encontradas nos portais dos municípios analisados. Tais vulnerabilidades tem o potencial de permitir que elementos mal-intencionados causem impactos negativos relevantes à continuidade do serviço. Essa pesquisa indicou, também, como corrigir os problemas identificados, o que pode permitir aos gestores públicos efetuarem ações que visem minimizar falhas de segurança e a adoção de estratégias de segurança, bem como a implantação de uma política de segurança da informação.

Palavras-Chave: Governo Eletrônico. Gestão da segurança da informação. *Scanner* de vulnerabilidades.

ABSTRACT

Electronic government can be characterized as the use of Information and Communication Technologies by public administration as support for internal government processes and the delivery of government products and services to citizens and industry in a fast and efficient way. It is essential that e-government prevents unauthorized access to ensure that Integrity, Availability and Confidentiality, basic principles of information security, are protected from electronic threats on the Internet. These threats place information assets at constant risk by taking advantage of the various vulnerabilities in the virtual environment where e-government is inserted. Thus, this research aimed to analyze the possible vulnerabilities in e-government portals of the municipalities of Paraíba State. The 50 municipalities that represent the largest share of the Gross Domestic Product (GDP) of the state of Paraíba were considered as the research population. From these, it was possible to analyze the portals of 40. This research was characterized as a descriptive research, with a Quantitative approach. In order to collect data, we used Nestparker software, a vulnerability scanner whose function is to track and identify vulnerabilities in Web applications. As a result, 822 vulnerabilities were found, of which 15% are Critical and 15% High Criticality. In addition, 10% of the vulnerabilities were classified as Medium Criticality, which, in addition to other vulnerabilities with higher impacts, represents a scenario with more than 40% vulnerabilities found in the portals of the municipalities analyzed. Such vulnerabilities have the potential to allow malicious elements to negatively impact the continuity of the service. In addition to identifying the vulnerabilities of electronic security in e-government portals in the State of Paraíba, this research indicated how to correct the identified problems, which allows public managers to take actions that aim to minimize security breaches and the adoption of security strategies as well as the implementation of an information security policy.

Keywords: Electronic Government. Information security management. Vulnerability scanner.

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os avanços nas Tecnologias de Informação e Comunicação (TIC) permitiram o desenvolvimento de diversas aplicações, tais como o comércio eletrônico (*e-commerce*), a aprendizagem eletrônica (*e-learning*) e o governo eletrônico (*e-egovernment*) (GUPTA; DASGUPTA; GUPTA, 2008). Sendo objeto de estudo dessa pesquisa, o governo eletrônico pode ser caracterizado como o uso e a aplicação das TIC, pela administração pública, com o intuito de racionalizar e integrar fluxos de trabalho e processos, conduzindo de maneira eficiente as informações e os serviços sob sua responsabilidade e atendendo às demandas da sociedade (UNITED NATIONS, 2014).

O desenvolvimento das TIC provoca alterações na dinâmica do governo com a sociedade, melhorando a organização do setor público, facilitando a comunicação com a sociedade, proporcionando outras maneiras de desenvolver a economia (FREIRE; STABILE, 2013) e se transformando em um instrumento de desenvolvimento sustentável (UNITED NATIONS, 2014).

Apesar de se utilizar das TIC, o governo eletrônico deve ser mais que o simples acesso à Internet, pois segundo a *Organization for Economic Cooperation and Development* (OECD, 2003), a prestação de serviços *on-line* ou a automação das rotinas de trabalho, pois deve ser encarado como uma iniciativa que busque o redesenho das estruturas burocráticas da administração pública a fim de que essa atinja os objetivos do papel do Estado (KENNEDY; COUGHLAN; KELLEHER, 2012), devendo envolver: i) mudanças nos fundamentos de funcionamento do governo e sua estrutura burocrática; ii) interação direta com os cidadãos, empresas, fornecedores e clientes internos dentro do governo e iii) a busca pela contínua eficiência da administração pública em atender as demandas da sociedade (DAMIAN; MERLO, 2013).

A implantação de um sistema de governo eletrônico traz vantagens tanto à Administração Pública ao facilitar a execução de suas atividades como a prestação de serviços e informações de caráter público, estabelecendo os objetivos de boa governança (OECD, 2003), como aos demandantes do serviço público, pois se torna mais cômodo e célere o acesso às informações e serviços de responsabilidade do governo, permitindo maior participação da sociedade ao desenvolver canais de

comunicação entre aqueles e seus governantes (FANG, 2002; IBRAHIM; ZAKARIA, 2015).

O Banco Mundial (2015) destaca como principais vantagens da implementação do governo eletrônico: a redução dos custos das atividades, pois o atendimento eletrônico tem custos bastante reduzidos quando comparados ao atendimento presencial; a promoção do desenvolvimento econômico, pois simplifica as relações entre governo e setores produtivos; a melhoria da transparência, pois ao tornar as informações acessíveis de maneira fácil e rápida, possibilita a fiscalização por parte da sociedade; a melhoria na prestação de serviços, pois serviços on-line possibilitam a redução da burocracia e aumento na qualidade dos serviços em tempo, conteúdo e acessibilidade.

A necessidade de uma reforma administrativa que reduzisse a burocracia dos processos administrativos e tornassem mais transparente e eficiente as ações do governo, introduzindo mecanismos de controle e fiscalização do Estado, propiciou o desenvolvimento do Programa de Governo Eletrônico brasileiro (PRADO, 2009). Nesse contexto de reforma estatal foram desenvolvidas as duas principais contribuições para a criação das políticas de estruturação do governo eletrônico no Brasil: a “Proposta de Política de Governo Eletrônico para o Poder Executivo Federal”, de autoria do Grupo de Trabalho Interministerial para o tema Tecnologia da Informação (GTTI) e a publicação do “Livro Verde - Sociedade da Informação no Brasil”, encomendado pelo Ministério da Ciência e Tecnologia.

O GTTI se encarregou de estipular as diretrizes do Programa de Governo Eletrônico destacando temas relacionados à necessidade da melhoria e ampliação dos serviços aos cidadãos, o desenvolvimento da transparência nas ações do governo e a melhoria na gestão interna. Outro ponto sinalizado pelo GTTI foi a necessidade de adequação do arcabouço jurídico, com a edição de normas e leis que facilitassem a implantação do programa de governo eletrônico.

O Livro Verde (2000) teve como objetivo o desenvolvimento de ações que fomentassem e popularizassem à utilização das Tecnologias da Informação e Comunicação, como forma de impulsionar a inclusão social de toda a população a fim de se adequarem à essa nova Sociedade Digital. Para isso, estipulou sete linhas de ações a serem adotadas para alcançar o objetivo do programa, compartilhando a responsabilidade dessas ações entre o governo, a iniciativa privada e a sociedade civil. Dentre as ações adotadas, destacam-se a: i) universalização do acesso do

cidadão aos serviços prestados pelo Governo, ii) a integração entre os sistemas, redes e bancos de dados da administração pública e iii) a abertura de informações à sociedade, por meio da Internet.

A necessidade de reforma do estado aliada ao desenvolvimento das TIC propiciou a expansão do governo eletrônico, possibilitando à Administração Pública criar maneiras de atender com eficiência, rapidez e transparência, as demandas da sociedade e dos próprios órgãos governamentais ao permitir que parte dessas requisições fosse realizada por meio eletrônico, facilitando o acesso à informação e serviços, sem a necessidade da presença física.

De acordo com o *Government Accountability Office* (GAO, 2015), o avanço das TIC fez crescer a dependência do Governo Federal pela utilização de sistemas informatizados para realizar operações, processar, manter e relatar informações essenciais onde o governo eletrônico encontra na *Internet* seu principal canal de divulgação e comunicação com a sociedade. Conforme Mandarino Junior e Canongia (2010), a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos.

A *Internet*, por proporcionar conectividade em tempo real, expandiu fortemente o volume transacionado de informações disponíveis, mas, ao mesmo tempo, fez crescer a preocupação com o tráfego de informações que circulam por meio eletrônico e sua adequada segurança (CARVALHO, 2011). A preocupação com a segurança da informação é essencial para prevenir a perda de recursos; o uso não autorizado ou inadequado, a divulgação ou alteração de informações confidenciais e a interrupção das atividades das organizações (GAO, 2015).

É nesse cenário conturbado que o objeto de estudo dessa pesquisa, o governo eletrônico, será analisado sob a ótica da segurança da informação. Conforme descreve a *International Standards Organization* (ISO/IEC 27000, 2014), a segurança da informação refere-se a proteger a informação de qualquer tipo de ameaça, procurando preservar a integridade, a disponibilidade e a confidencialidade da informação que são as três características fundamentais que definem o valor da informação (WHITMAN; MATTORD, 2011). O constante avanço de máquinas e sistemas de informação, além do aumento crescente de ameaças tecnológicas, torna imprescindível que o governo explore e estimule outras ideias para serem

discutidas e integradas ao tema segurança da informação no intuito de assegurar as características fundamentais da segurança e o valor da informação.

Os sistemas utilizados por agências federais são muitas vezes repletos de vulnerabilidades de segurança tanto conhecidas como desconhecidas. O aumento da interconectividade entre redes públicas e privadas, e a crescente complexidade dessas interconexões, com tecnologias diversificadas e muitas vezes dispersas geograficamente, aumenta a dificuldade em proteger a informação fazendo com que órgãos governamentais sejam suscetíveis a maiores riscos devido ao tamanho da sua infraestrutura (GAO, 2015).

As vulnerabilidades presentes nos sistemas de informação representam uma falha na concepção de um processo ou programa e essa fragilidade se torna um ambiente propício a ser explorada por ameaças e/ou atacantes. Tome como exemplo o Programa de Governo Eletrônico que se utiliza de páginas na *Web* para a prestação de informações e serviços, páginas essas que podem ser compostas de informações de fontes simultâneas de todo o mundo. Basta apenas que uma dessas fontes seja comprometida para que um ataque eletrônico seja rapidamente propagado e afete muitos outros usuários. As vulnerabilidades na infraestrutura tornam a *Web* vulnerável ao ataque (SYMANTEC, 2009).

O número de ataques virtuais contra governos e organizações comerciais continua a crescer em frequência e gravidade (PONEMON INSTITUTE, 2015) e mostram uma tendência no aumento de ataques cada vez mais sofisticados e prejudiciais, pois na falta de programas e políticas adequadas de segurança, os governos tem experimentado um grande número de incidentes que envolvem perda de dados, roubos e invasões. O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.Gov), responsável pela notificação e tratamento de incidentes da Administração Pública Federal, relatou mais de 5.000 incidentes ocorridos apenas no primeiro semestre de 2016.

Graves vulnerabilidades e falhas no controle de segurança da informação tem representado uma ameaça constante aos ativos federais que correm o risco de serem acessados por pessoas não autorizadas, podendo ser destruídos, modificados, ou ainda, causar a interrupção das atividades da Administração Pública. Os órgãos governamentais não estão suficientemente protegidos para impedir as ameaças cibernéticas, pois conforme apontado pelo Tribunal de Contas

da União (TCU) (BRASIL, 2014), o nível de adoção das práticas de segurança da informação, de forma geral, ainda está distante de um cenário satisfatório para a Administração Pública Federal (APF).

O levantamento do TCU, em 2014, apurou que 87% das organizações da Administração Pública Federal disponibilizam algum tipo de serviço por meio da *Internet*, o que aponta a tentativa de facilitar e melhorar a relação entre governo e demais interessados. Apesar disso, o TCU também destacou que 61% das organizações da APF não apresentam capacidade adequada de governança e gestão de TI, ou seja, as vulnerabilidades decorrentes da inadequada gestão de TI revela-se um ambiente propício para ameaças e ataques cibernéticos, expondo a APF a diversos riscos como indisponibilidade de serviços e perda de integridade de informações.

As informações disponíveis no Programa de Governo Eletrônico devem ser resguardadas a fim evitar qualquer acesso não autorizado que coloque em risco ou prejudique as atividades do governo ou ainda possibilite a revelação de dados de seus usuários. As vulnerabilidades presentes em sistemas eletrônicos ameaçam a identidade, privacidade e dados de seus usuários.

O governo eletrônico ao utilizar-se, em especial, da *Internet* para disponibilizar serviços eletrônicos às pessoas, trouxe facilidade, rapidez e transparência, mas, por outro lado, a insegurança das redes e sistemas utilizados para o tráfego dos dados, devido às suas vulnerabilidades, criou um problema relevante para a segurança dos serviços e informações podendo abalar a confiança dos cidadãos na capacidade do governo eletrônico em proteger adequadamente as informações que dispõe e/ou solicita de seus usuários.

Diante das exposições acima, percebe-se a importância do governo eletrônico em facilitar o acesso a serviços e informações demandados pela sociedade, bem como se destacam as preocupações relativas às vulnerabilidades presentes em sistemas e redes, utilizados pelo governo eletrônico, que podem ser alvo de ameaças e ataques cibernéticos. Dessa maneira, essa pesquisa propõe-se a responder a seguinte questão de pesquisa: **Quais as possíveis vulnerabilidades existentes em portais de governo eletrônico em municípios do Estado da Paraíba?**

Para responder a essa questão foi escolhida em uma amostra intencional, um conjunto de portais de governo eletrônico referentes aos municípios do Estado da

Paraíba, e, nesses, foi aplicado uma análise que permitiu identificar as vulnerabilidades computacionais. Cabe ressaltar que “portais de governo eletrônico” referem-se às páginas eletrônicas localizadas na *Internet* nas quais os governos mostram sua “identidade, seus propósitos, suas realizações e possibilitam a concentração e disponibilização de serviços e informações, o que facilita a realização de negócios e o acesso à identificação das necessidades dos cidadãos” (PINHO, 2008, p. 473). Dessa maneira, esse estudo terá seus procedimentos orientados pelos seguintes objetivos:

1.1 OBJETIVOS

Sendo a temática desse estudo verificar a segurança da informação em portais de governo eletrônico em municípios do Estado da Paraíba, indicam-se a seguir os objetivos que orientaram a pesquisa:

1.1.1 Objetivo Geral

O objetivo geral é analisar as possíveis vulnerabilidades existentes em portais de governo eletrônico dos municípios do Estado da Paraíba.

1.1.2 Objetivos Específicos

Para que o objetivo geral seja atingido, foram definidos os seguintes objetivos específicos:

a) Identificar os portais de governo eletrônico em municípios do Estado da Paraíba que serão analisados por meio de pesquisa realizada na *Internet* para verificar os portais existentes;
b) aplicar o *scanner* de vulnerabilidade, Netsparker, nos portais de governo eletrônico em municípios identificados do Estado da Paraíba;
c) descrever as possíveis soluções para a correção das vulnerabilidades identificadas nos portais de governo eletrônico em municípios do Estado da Paraíba.

1.2 JUSTIFICATIVA

As propostas para a implantação de um sistema de governo eletrônico se destinam a aumentar o nível de eficiência da Administração Pública, onde a aplicação bem sucedida dessas iniciativas fornece a prestação de melhores serviços governamentais e informações à sociedade, além de ampliar a participação dos cidadãos no processo de tomada de decisão (ALMARABEH; ABUALI, 2010). Ainda assim, conforme o *Center for Democracy & Technology* (CDT, 2002), a implementação de um programa de governo eletrônico é dispendioso e requer planejamento, liderança, colaboração, vontade política, apoio da população e seus potenciais benefícios só serão alcançados por meio da compreensão dos obstáculos existentes em sua implementação (ALMARABEH; ABUALI, 2010).

De acordo com Ebrahim e Irani (2005), um dos maiores desafios na estratégia de governo eletrônico é a necessidade de garantir segurança, privacidade, confidencialidade e confiabilidade dos dados de seus usuários. O êxito na implementação de um programa de governo eletrônico consiste em demonstrar, a todos os interessados, a confiabilidade de seu projeto, considerando a segurança das informações de seus usuários, bem como sua privacidade, garantindo que os sistemas de informação estejam devidamente protegidos contra acessos indevidos (CDT, 2002; FANG, 2002).

Um projeto de governo eletrônico será considerado eficiente quando, conforme Ebrahim e Irani (2005), todos os seus usuários, incluindo agências governamentais, empresas privadas e cidadãos, se sentirem confortáveis na utilização dos meios eletrônicos para a realização de operações pessoais.

A fim de garantir essa confiabilidade, o governo deve estipular diretrizes e normas, criando uma política de segurança da informação, que necessitará de revisão periódica, para assegurar a sua adequação às exigências do contexto de serviços eletrônicos que se apresente (IBRAHIM; IRANI, 2005).

Quando um atacante invade um sistema, ele se aproveita das vulnerabilidades em procedimentos, tecnologia ou gerenciamento (ou a combinação desses fatores), permitindo acesso ou ações não autorizadas. Dessa maneira, o governo deverá, ao projetar o sistema de governo eletrônico, adotar uma política clara e objetiva de segurança da informação, de modo que a privacidade e a

segurança dos usuários sejam mantidas e as ameaças digitais não possam prejudicar o sistema.

Esse estudo justifica-se pela necessidade de verificar se a Administração Pública adota medidas de segurança, em seus portais de governo eletrônico, capazes de reduzir as vulnerabilidades existentes e que sejam compatíveis com a importância das informações e serviços sob sua responsabilidade. Essa verificação deve ser realizada constantemente, pois, dessa maneira, a adequada proteção dos dados e sistemas utilizados pela Administração Pública preservará a privacidade de seus usuários e garantirá a confiabilidade nos serviços e informações prestados eletronicamente.

Para fins de delimitação, já que não será possível analisar a vulnerabilidade em todos os portais de governo eletrônico brasileiro, esse estudo terá como escopo os portais de governo eletrônico de 50 municípios do Estado da Paraíba, considerando suas respectivas participações no Produto Interno Bruto (PIB) do Estado. Segundo o Instituto de Desenvolvimento Municipal e Estadual (IDEME, 2016), as cinco cidades que apresentaram maior participação no PIB do Estado da Paraíba foram João Pessoa (32,0%), Campina Grande (14,1%), Cabedelo (4,5%), Santa Rita (4,1%) e Patos (2,5%). Juntas, essas cidades representam mais da metade de toda a riqueza produzida no estado da Paraíba. Quando se analisa os 50 primeiros municípios que participam na composição do PIB, observa-se que representam 83,4% do Produto Interno Bruto do Estado da Paraíba.

A escolha dos sites governamentais dos municípios do Estado da Paraíba, com maior participação no PIB, se deve, primeiro, em razão do Mestrado Profissional em Gestão em Organizações Aprendentes (MPGOA) ser vinculado à Universidade Federal da Paraíba (UFPB) e como tal, tanto o Programa quanto a Instituição buscam desenvolver pesquisas que agreguem conhecimento para a comunidade acadêmica, mas que também seja útil ao desenvolvimento da região em que está inserida, seja por meio do ensino, extensão ou pesquisa. Segundo, por ser uma contrapartida social, buscando contribuir de forma prática com a gestão das organizações, ao analisar, em sites do governo, as possíveis vulnerabilidades que comprometam a segurança, possibilitando aos gestores públicos a adoção de medidas necessárias para a eliminação dos problemas.

Essa pesquisa foi dividida em seções, a saber: a Introdução que é tratada na primeira seção, na segunda é trabalhado o referencial teórico, na terceira a

metodologia, na quarta seção é apresentado e analisado os resultados, em seguida as considerações finais e por fim, as referências, seguidos dos apêndices.

2 REFERENCIAL TEÓRICO

Faz parte do referencial teórico, os tópicos de governo eletrônico e segurança da informação. Dessa maneira, esta seção expõe definições e conceitos que construirão o referencial teórico e orientará o estudo. Inicialmente, apresentam-se as definições do que se considera governo eletrônico, os benefícios de sua implementação, as formas de interação com os usuários e, por fim, os estágios de implementação de um sistema de governo eletrônico. Também há um breve histórico da implementação do governo eletrônico no Brasil e seu desenvolvimento. Por fim, apresentam-se os conceitos de segurança da informação e as ameaças, vulnerabilidades e ataques presentes em meio eletrônico. Os conceitos apresentados não têm como objetivo explorar todas as facetas destes tópicos presente na literatura, mas oferecer referencial para subsidiar as análises efetuadas para o estudo.

2.1 GOVERNO ELETRÔNICO – uma visão geral

A revolução na inovação das Tecnologias de Informação e Comunicação (TIC), em especial a expansão da Internet, no final dos anos 1990, possibilitou à sociedade exercer pressão sobre os governos com o objetivo de esses adotarem uma administração pública mais eficiente, economizando recursos, atuando de forma transparente e facilitando o acesso aos serviços e informações demandados. Conforme Freire e Stabile (2013, p. 48), o desenvolvimento das TIC impacta diretamente no funcionamento dos governos e nas dinâmicas sociais, econômicas e políticas das sociedades. Dessa forma, a partir da evolução das TIC, a ideia e o termo “governo eletrônico” ganha destaque, pois se espera que seu desenvolvimento possibilite uma mudança nas características de interação entre governo e sociedade, tornando possível a prestação de serviços, de maneira rápida eficiente, sem a necessidade da presença física.

O governo eletrônico pode ser caracterizado como o uso de uma variedade de tecnologias de informação e comunicação pelo poder público, em especial a Internet, como meio de facilitar a prestação de serviços e informações de interesse dos cidadãos e empresas (BURN; ROBINS, 2003; WEST, 2004; GRÖNLUND, 2004;

AKMAN *et al*., 2005), tornando mais transparente e participativa as relações entre esses atores (DAMIAN; MERLO, 2013).

A *Organization for Economic Co-operation and Development* (OECD, 2003) considera haver várias definições de governo eletrônico e que esses diferentes conceitos refletem as prioridades nas estratégias de cada governo. Para a OECD essas definições podem se dividir três grupos da seguinte maneira:

i) o governo eletrônico é o uso da Internet, pelo governo, para a prestação de serviços;

ii) o governo eletrônico é a utilização das TIC, pelo governo, para a prestação de serviços incluindo outros aspectos da atividade do governo;

iii) o governo eletrônico é a capacidade de transformar a administração pública, pela adoção e utilização das TIC, em uma nova forma de governo.

A definição adotada pela OECD considera o governo eletrônico como o uso das TIC, em especial a Internet, como uma ferramenta para atingir um governo mais eficiente.

As Nações Unidas (2014, p. 2) citam que o governo eletrônico pode ser considerado como o uso e aplicação das tecnologias da informação na administração pública para “racionalizar e integrar os fluxos de trabalho e processos, para gerir eficazmente os dados e informações, e melhorar a prestação de serviços públicos, bem como ampliar os canais de comunicação para envolvimento e capacitação das pessoas” (tradução nossa).

Uma definição mais ampla é dada pelo Banco Mundial (2015) ao ressaltar que o governo eletrônico refere-se à utilização, pela administração pública, de tecnologias de informação, que têm a capacidade de transformar as relações com os cidadãos, empresas e o próprio governo. Essas tecnologias auxiliam diversos propósitos, tais como: melhor prestação de serviços públicos aos cidadãos, interações melhoradas com o comércio e a indústria e a maior participação da sociedade, por meio do acesso à informação, impelindo uma gestão mais eficiente por parte do governo.

Garcia (2006) define que governo eletrônico vai além da capacidade de disponibilizar serviços aos cidadãos de maneira eletrônica, sendo também a possibilidade da:

> dinamização dos processos governamentais (jurídico-legistativos, de políticas públicas, etc.) de forma integrada (interoperável), ou seja, envolvendo todas as instâncias governamentais, privadas ou não-

> governamentais, através das modernas tecnologias de informação e comunicação, objetivando a integração, transparência, governabilidade e a democracia (GARCIA, 2006, p. 81).

Caldas (2007, p. 38), corrobora com a ideia da necessidade de transformação na estrutura tradicional da administração pública antes da implementação do governo eletrônico, pois para o autor é um projeto que busca “se colocar na direção da capacitação do setor público para enfrentar desafios que se apresentam à sociedade da Era Digital. Em um mundo conectado, é apresentado como um modelo de competência e de governança para o século XXI”. Kennedy, Coughlan e Kelleher (2010) também consideram que governo eletrônico não pode ser definido apenas como a prestação de serviços públicos e informações *on-line,* mas sim como uma iniciativa transformadora na administração pública, permitindo a essa, o redesenho de sua estrutura burocrática onde os problemas não são de natureza tecnológica e sim organizacional. Ainda segundos os autores, a mudança nos processos e estruturas governamentais é que possibilita os maiores benefícios pelo uso das TIC.

Parece haver consenso entre pesquisadores e organizações ao considerar governo eletrônico como um governo que se utiliza de tecnologias de informação e comunicação para oferecer aos cidadãos e às empresas a oportunidade de interagir e realizar negócios com o governo, usando diferentes meios de comunicação. O governo eletrônico possibilita a transformação no modo de interação entre a administração pública e seus usuários.

Conforme Teo, Srivastava e Jiang (2008), o governo eletrônico tem sido reconhecido como um meio de transformação da governança pública, tendo a capacidade de modificar a forma de disponibilização dos serviços públicos, reduzindo a burocracia e reestruturando as estruturas administrativas do governo, permitindo a prestação de serviços de maneira eficiente, transparente e responsável. Além disso, passa a ser uma poderosa ferramenta para apoiar os cidadãos e assegurar que os objetivos da boa governança sejam alcançados (SILVA, 2013).

2.1.1 Benefícios do Governo Eletrônico

Entre os benefícios da implantação de um sistema de governo eletrônico Silcock (2001) acrescenta que o governo eletrônico beneficia a população e os parceiros de negócio, pois consegue criar um novo modelo de serviço público em

que todas as organizações públicas se comprometem a desenvolver um serviço de qualidade, integrado e menos burocrático. Conforme a OECD (2003), o governo eletrônico auxilia a administração pública na melhor execução de suas atividades por meio da consolidação dos objetivos de boa governança.

Outros benefícios proporcionados pelo governo eletrônico aos cidadãos e empresas, são a comodidade e celeridade no acesso às informações e serviços do governo, ocasionando economia de tempo, assim como a melhoraria da qualidade dos serviços e maiores oportunidades de participação nas instituições e processos democráticos (FANG, 2002; IBRAHIM; ZAKARIA, 2015). Gupta, Dasgupta e Gupta (2008) e Sultan, AlArfaj e AlKutbi (2012) observam que a implantação do governo eletrônico pode trazer maior produtividade das atividades públicas, melhorar a satisfação dos cidadãos e fomentar o crescimento econômico pela redução de custos. A Implantação de sistemas de governo eletrônico pode melhorar a capacidade da administração pública, mas os efeitos estimados variam de acordo com o tipo e funcionalidade do sistema de governo eletrônico adotado, da atividade do governo e do contexto de cada país (KOCHANOVA; HASNAIN; LARSON, 2016).

Embora uma das características mais importantes do governo eletrônico seja a entrega rápida, fácil e eficiente de serviços e informações aos seus usuários, por meio das TIC, cabe salientar que um projeto de governo eletrônico vai além desses benefícios. Segundo Ebrahim e Irani (2005), o governo eletrônico possibilita o desenvolvimento de conexões estratégicas entre as próprias organizações do setor público, fomentando a cooperação mútua, facilitando a execução das estratégias, transações e políticas do governo, além da melhor utilização e funcionamento dos processos governamentais.

O Banco Mundial (2015) expõe algumas das principais vantagens e benefícios, para a sociedade, da implementação de um sistema de governo eletrônico, sendo elas:

- **Redução de custos**: serviços on-line diminuem os custos de processamento de muitas atividades quando comparada à maneira tradicional de atendimento presencial;
- **Promoção do desenvolvimento econômico:** as TIC permitem aos governos a simplificação das relações com as empresas e a redução das medidas administrativas necessárias para dar cumprimento às obrigações regulatórias;

- **Melhoraria da transparência:** o governo eletrônico possibilita o aumento da transparência dos processos de tomada de decisão ao tornar as informações publicamente acessíveis de maneira rápida, permitindo aos cidadãos o acompanhamento e fiscalização dos atos da gestão pública;
- **Melhoraria na prestação de serviços:** a prestação de serviços do governo, no processo tradicional, provoca insatisfação tanto a cidadãos quanto a empresas pela demora e falta de transparência. A disponibilização de serviços governamentais em rede reduz a burocracia e aumenta a qualidade dos serviços em termos de tempo, conteúdo e acessibilidade.

As Nações Unidas (2014, p. 3, tradução nossa) argumentam que o governo eletrônico é considerado um meio para o desenvolvimento de todos, se constituindo em uma poderosa ferramenta a disposição dos governos, que, “se aplicada de forma eficaz, pode contribuir substancialmente para a erradicação da pobreza extrema, proteger o ambiente e promover a inclusão social e oportunidades econômicas para todos”.

2.1.2 Formas de Interação

Santos e Reinhard (2012, p. 123-124) consideram que as atividades características do governo eletrônico não se restringem somente à prestação eletrônica de informações e serviços, pois também inclui a:

> - regulamentação das redes de informação, envolvendo principalmente governança, certificação e tributação;
> - prestação de contas públicas, transparência e monitoramento da execução orçamentária;
> - ensino à distância, alfabetização digital e manutenção de bibliotecas virtuais;
> - difusão cultural com ênfase nas identidades locais, fomento e preservação das culturas locais;
> - e-procurement, isto é, aquisição de bens e serviços por meio da Internet, como licitações públicas eletrônicas, pregões eletrônicos, cartões de compras governamentais, bolsas de compras públicas virtuais e outros tipos de mercados digitais para bens adquiridos pelo governo;
> - estímulo aos negócios eletrônicos, através da criação de ambientes de transações seguras, especialmente para pequenas e médias empresas.

Considerando o conjunto de atribuições e atividades que podem abranger a implantação de um governo eletrônico, é possível, também, distinguir três grupos e identificar suas diferentes relações com o governo. Comumente são citados três

tipos de usuários de um sistema de governo eletrônico, (TAKAHASHI, 2000; YILDIZ, 2007; NORRIS; REDDICK, 2013), e, conforme Takahashi (2000, p. 69), os "envolvidos nos serviços governamentais são o próprio Governo ("G"), Instituições Externas ("B", de *business*), e o Cidadão ("C")".

De acordo com Fang (2002), semelhante ao princípio do comércio eletrônico, que permite às empresas realizarem transações entre elas, com mais eficiência e aproximando os clientes do negócio, a administração pública busca, com a implantação de um sistema de governo eletrônico, tornar a interação mais amigável e eficiente entre governo e cidadãos (G2C), governo e empresas (G2B) e entre agências governamentais (G2G). Para Takahashi (2000) existem cinco tipos de relações entre o governo e seus usuários, sendo elas: "Governo com Governo" (G2G); "Governo com as Empresas e Empresas com o Governo" (G2B/B2G) e, por fim, "Governo com o Cidadão e Cidadão com o Governo" (G2C/C2G).

2.1.2.1 Governo com o Cidadão (G2C)

A relação do Governo com o Cidadão (G2C) facilita a interação desse com o aquele, que é o objetivo principal do governo eletrônico. O cidadão realiza transações de maneira mais rápida e menos burocrática, tais como pagamento de impostos e taxas, impressão de documentos, obtenção de certidões negativas, renovações, consulta de benefícios, cadastramentos, entre outras. Com essas iniciativas o Governo se esforça em melhorar o acesso à informação pública usando sites e outros meios eletrônicos. A implementação dessas iniciativas tem como objetivo desenvolver um espaço virtual onde os cidadãos possam realizar diversas tarefas, especialmente aquelas que envolvam vários departamentos governamentais, sem a necessidade de o cidadão entrar em contato com cada departamento individualmente. Takahashi (2000, p. 77) reforça os benefícios da implementação de sistemas de governo eletrônico ao dizer que:

> [...] as aplicações têm adquirido uma tendência natural [...] a serem mais próximas de atendimento ao cidadão comum, em locais específicos para tal e também em locais de acesso público [...]. Um exemplo muito interessante nessa classe de aplicações é o de serviços de obtenção de documentos e atestados, abertura de empresas, pagamento de impostos etc., que têm vicejado em diversos estados sob diferentes nomes (exemplo: Serviço de

> Atendimento ao Cidadão, Poupa-Tempo etc.) e que, aliás, foram a inspiração de alguns serviços similares em outros países, inclusive na União Européia.

A relação G2C tem como princípio oferecer um governo mais eficiente e eficaz por meio da melhoria contínua na prestação de serviços, de maneira menos burocrática, à população e com resultado mais confiáveis (SINGH; PARIHAR, 2015).

2.1.2.2 Governo com as Empresas (G2B)

A relação do Governo com as Empresas (G2B) está relacionada pela aquisição, por parte do governo, de bens e serviços de fornecedores do setor privado contratados por meio de transações eletrônicas. Essa relação se dá por meio da divulgação de Editais de compras públicas, pregões eletrônicos, informações sobre importação e exportação, nota fiscal eletrônica, etc. As empresas, com o objetivo de reduzir custos de operação, preferem realizar suas atividades como vendas, compras e contratações por meios eletrônicos.

Pela experiência positiva nas transações *on-line* realizada entre empresas (B2B) que tem como objetivo a diminuição de custos, tanto o governo quanto as empresas querem executar e estender essas negociações por meio eletrônico, já que a demanda por eficiência e menores custos se aplica tanto ao setor privado quanto à administração pública (SINGH; PARIHAR, 2015). Um exemplo de relação do governo com empresas por meio de uma aplicação eletrônica é o sistema ComprasNet do Ministério do Planejamento que tem como objetivo disponibilizar à todos os interessados, informações referentes às licitações e contratações promovidas pelo Governo Federal, bem como permitir a realização de processos eletrônicos de aquisição. De acordo com Takahashi (2000, p. 76), esse tipo de iniciativa torna-se:

> [...] fundamental para a modernização e a desburocratização dos processos de aquisição, tendo como objetivo principal dotar a sociedade de um instrumento que utilize as inovações tecnológicas da Internet, para oferecer facilidades aos fornecedores e, ao mesmo tempo, gerar economia para o Governo Federal, por intermédio da adoção de novos padrões de qualidade e produtividade.

Sendo um importante usuário do governo eletrônico, as instituições privadas se beneficiam com seu desenvolvimento. Quanto maior a eliminação da burocracia

processual e governamental, melhor a interação entre governo e setor privado, o que privilegia o desenvolvimento de setores produtivos, consequentemente desenvolvendo o país.

2.1.2.3 Governo com o Governo (G2G)

A relação do Governo com o Governo (G2G) refere-se às transações e interações realizadas internamente em uma instituição pública ou entre agências estatais, podendo ser inclusive entre agências de diferentes esferas de governo (federal, estadual ou municipal) ou de Poderes (Executivo, Legislativo ou Judiciário). Um dos seus objetivos é aumentar a eficiência, eficácia e a efetividade da ação estatal. Como exemplo, o Comitê Gestor da Internet no Brasil (CGI.br, 2014) cita a criação de sistemas para a gestão de projetos públicos ou para a administração de recursos humanos de todo o governo federal, como o Siape - Sistema Integrado de Administração de Recursos Humanos do Poder Executivo Federal.

De acordo com Singh e Parihar (2015), cada um desses grupos apresenta diferentes motivos e necessidades específicas para se relacionarem com o governo. Apesar disso, alguns objetivos comuns incluem a melhoria da eficiência, confiabilidade e qualidade dos serviços para os respectivos grupos. Ainda segundo os autores, o grupo G2G pode ser considerado como o principal grupo de sustentação do governo eletrônico, pois se supõe que um sistema de governo eletrônico deva ser capaz de atender com qualidade e eficiência às próprias necessidades do governo e demais esferas da administração pública, antes de introduzir e disponibilizar aplicações eletrônicas para cidadãos e empresas.

2.1.3 Estágios do Governo Eletrônico

Apesar dos benefícios esperados pela utilização de um sistema de governo eletrônico, diversos são os desafios em sua implantação. De acordo com Almarabeh e Abuali (2010), a implantação de um governo eletrônico é um processo contínuo, e na maioria das vezes seu desenvolvimento é feito em estágios, mas nem todos os governos chegarão a todos os estágios. Além do mais, esses estágios apresentam diferentes modelos, podendo ser mais ou menos estágios a depender do

entendimento de cada autor ou organização. O Quadro 1 exemplifica alguns desses modelos:

Quadro 1 - Modelo de estágios do governo eletrônico

	ESTÁGIOS	CARACTERÍSTICAS
BANCO MUNDIAL	Divulgação	Países em desenvolvimento, em geral, podem iniciar o processo de governo eletrônico por meio da publicação de informações *on-line*, começando com regras, regulamentos, documentos e formulários.
	Interação	O governo eletrônico envolve os cidadãos no processo de governança por meio da interação com os formuladores de políticas públicas em todos os níveis de governo.
	Transação	Nesse estágio é desenvolvida a criação de sites que permite aos usuários realizar transações on-line.
LAYNE e LEE	Catálogo	Oferece algumas informações básicas através de web sites com pouca atualização.
	Transação	Amplia a capacidade do estágio anterior ao permitir que os cidadãos façam algumas simples transações on-line como preenchimento de formulários do governo.
	Integração Vertical	Inicia a transformação dos serviços do governo antes de automatizar seus processos existentes. Esse estágio se concentra na integração de funções do governo em diferentes níveis, como governos locais e governos estaduais.
	Integração Horizontal	Dedica-se à integração das diferentes funções de vários sistemas independentes de modo a fornecer aos usuários um serviço unificado.
NAÇÕES UNIDAS	Presença Emergente	Um único ou poucos sites do governo, independentes entre si, fornecendo informações de maneira limitada e com poucas atualizações.
	Presença Aprimorada	Vários sites do governo fornecem informações dinâmicas e atualizadas regularmente.
	Presença Interativa	Sites do governo funcionando como um portal para conectar os usuários e prestadores de serviços onde a interação ocorre em um nível mais sofisticado.
	Presença Transacional	Os usuários têm a capacidade de realizar transações completas e seguras, como pagamento de multas trânsito, impostos e taxas por meio de cartão de crédito, bancário ou de débito.
	Presença em Rede	Os governos utilizam um único web site para servir de canal de comunicação em que os usuários podem ter de maneira imediata acesso a todos os tipos de serviços disponíveis.

Fonte: *United Nation Public Administration Network* (2010)

Conforme observado por Medeiros (2004, p. 34) os países que implantam o governo eletrônico podem estar posicionados em mais de um estágio, pois a:

> [...] categorização em cinco estágios mostra qual o percentual de serviços *on-line* que cada Administração Pública oferece em cada estágio. Por exemplo: os Estados Unidos, que possuem o maior índice de prontidão para governo eletrônico, utilizam em torno de 46% dos possíveis serviços transacionais *on-line* (Estágio IV das Nações Unidas). A Suécia, por sua vez, segunda colocada nesse mesmo índice, utiliza apenas 20% do potencial transacional em serviços na *web*.

O sucesso do governo eletrônico exige mudanças nos fundamentos de funcionamento do governo e sua estrutura burocrática. O governo eletrônico não é apenas sobre a automação de procedimentos, pois esses podem ser ineficientes, mas sobre a criação de novos processos e estruturas eficientes que facilitem as relações entre governo e sociedade. Para resultados positivos na implantação de um governo eletrônico é necessário que os governos transformem, radicalmente, a forma das operações da administração pública. Considerando a complexidade do setor público, todas as esferas governamentais devem extinguir procedimentos ultrapassados e estruturas burocráticas substituindo por estruturas flexíveis e adaptáveis às constantes mudanças de contextos organizacionais (WEERAKKODY; DHILLON, 2008; KENNEDY; COUGHLAN; KELLEHER, 2010).

O maior valor da implantação de um sistema de governo eletrônico está na capacidade da gestão pública poder repensar, reorganizar e reestruturar seus processos burocráticos, oriundos de ideias válidas no século passado, que hoje se mostram incapazes de atenderem às demandas da sociedade.

2.2 GOVERNO ELETRÔNICO NO BRASIL

Como já dito, a implementação de um programa de governo eletrônico requer mais que a simples automatização e disponibilidade eletrônica das informações e serviços existentes na administração pública, antes disso, necessita de uma ação cuidadosamente planejada com objetivos de curto, médio e longo prazo, pois envolve a reforma dos trabalhos administrativos, racionalização dos trabalhos redundantes e projetos desenvolvidos por diferentes agentes/órgãos públicos, além das possíveis revisões do arcabouço legal existente.

Entre as razões para explicar a popularização do termo governo eletrônico, no final dos anos 1990, está, conforme Prado, Ribeiro e Diniz (2012), o rápido avanço das Tecnologias de Informação e Comunicação (TIC) que transformou as relações entre indivíduos, indivíduos e organizações e indivíduos e sociedade. A segunda razão apresentada pelos autores foi a necessidade da modernização da administração pública, ou seja, tornar a administração pública mais simples e mais eficiente, diminuindo os encargos para a sociedade e permitindo maior transparência, acompanhamento e controle dos gastos públicos.

Conforme Prado (2009, p. 68) o surgimento do governo eletrônico está associado aos "movimentos de reforma do Estado, em especial na qualidade de um dos mais efetivos instrumentos de controle das contas públicas e de melhoria da eficiência dos processos governamentais". No Brasil, essa "modernização" da gestão pública foi diretamente influenciada, segundo Diniz *et al*. (2009, p. 26), como "[...] resultado do esgotamento do modelo de gestão burocrática e do modo de intervenção estatal" resultando na criação, em 1995, do Plano Diretor da Reforma do Estado, que segundo Pereira (1999, p. 6) foi criado para substituir a "atual administração pública burocrática, misturada a práticas clientelistas ou patrimonialistas, por uma administração pública gerencial, que adota os princípios da nova gestão pública [...]".

O Plano Diretor teve como objetivo, "criar condições para a reconstrução da administração pública em bases modernas e racionais" (BRASIL, 1995, p. 6) e, nesse sentido, criou diversos projetos para atingir tal intento, entre eles o "Rede do Governo" e o "Projeto Cidadão" que, segundo Mantovane (2012, p. 32), seriam as "primeiras referências ao futuro programa de governo eletrônico". Como exemplo, o projeto "Rede do Governo" teve como iniciativa desenvolver uma:

> [...] moderna rede de comunicação de dados interligando de forma segura e ágil a administração pública, permitindo assim um compartilhamento adequado das informações contidas em bancos de dados dos diversos organismos do aparelho do Estado, bem como **um serviço de comunicação (baseado em correios, formulários, agenda e "listas de discussão", todos eletrônicos**) de forma a poder repassar à sociedade em geral e aos próprios órgãos do governo, a maior quantidade possível de informação, contribuindo para melhor transparência e maior eficiência na condução dos negócios do Estado (BRASIL, 1995, p.65, grifo nosso).

Dentro desse contexto de reforma da Administração Pública, foi instituído, pelo Decreto Presidencial de 3 de abril de 2000, o Grupo de Trabalho Interministerial

para o tema Tecnologia da Informação (GTTI) com a finalidade de examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação.

2.2.1 Grupo de Trabalho Interministerial (GTTI)

A criação do GTTI pode ser considerada a primeira iniciativa de elaboração de uma política de “governo eletrônico” e seus trabalhos possibilitaram o “estabelecimento de um modelo conceitual de Governo Eletrônico, com ênfase na proposição de medidas para a promoção das novas formas eletrônicas de interação entre o governo e o cidadão” (BRASIL, 2002).

Esse Grupo de Trabalho era composto por representantes dos seguintes órgãos: i) Casa Civil da Presidência da República; ii) Ministério do Desenvolvimento, Indústria e Comércio Exterior; iii) Ministério da Ciência e Tecnologia; iv) Ministério do Planejamento, Orçamento e Gestão; v) Ministério das Comunicações; vi) Ministério da Justiça; vii) Gabinete de Segurança Institucional da Presidência da República; e viii) Secretaria de Comunicação de Governo da Presidência da República. Como observado por Prado, à composição do GTTI, representando diversos setores da estrutura governamental:

> [...] indicava que o programa não estava sendo visto apenas como uma questão de tecnologia, ainda mais se considerarmos que a coordenação não estava vinculada à área tecnológica, [...], mas sim diretamente à Presidência da Republica (PRADO, 2009, p. 76).

Os estudos e discussões realizados pelo GTTI resultaram em um “relatório de diagnóstico da situação da Infraestrutura e serviços do Governo Federal, as aplicações existentes e desejadas e a situação da legislação sobre o assunto”, levando o GTTI a publicar em 20 de setembro de 2000 a “Proposta de Política de Governo Eletrônico para o Poder Executivo Federal” (BRASIL, 2016a).

Esse documento estipulou como diretrizes do Programa Governo Eletrônico “a melhoria dos serviços prestados ao cidadão, a ampliação do acesso a serviços, a melhoria da gestão interna e a transparência e controle social sobre as ações de Governo” e apresentou as diversas iniciativas que já estavam em processo de implementação, mas ressaltou a “necessidade de uma política integrada e

abrangente [...] em direção à efetiva universalização do acesso às tecnologias da informação e aos serviços de interesse do cidadão" (BRASIL, 2002, p. 6-8). O documento também sinalizou a necessidade da revisão de leis e edição de normas e decretos com o propósito de viabilizar a implantação do programa. No Programa Sociedade da Informação (a ser visto em tópico posterior) Takahashi (2000, p. 73), também apontou que para atender "às necessidades geradas pelo emprego das tecnologias de informação e comunicação em aplicações de governo" as normas legais deveriam ser revistas.

Para dar seguimento às propostas do GTTI, foi criado, pelo Decreto Presidencial de 18 de outubro de 2000, o Comitê Executivo do Governo Eletrônico (CEGE) que tinha como objetivo a formulação de políticas, o estabelecimento de diretrizes e a articulação das ações voltadas para a implantação do programa de governo eletrônico (BRASIL, 2000a). Prado, Ribeiro e Diniz (2012) consideram que a atuação do CEGE foi essencial para o desenvolvimento do programa, pois segundo os autores, esse comitê demonstrou o compromisso do Governo Federal com a implantação e desenvolvimento do programa de governo eletrônico.

2.2.2 Sociedade da Informação – Livro Verde

A elaboração e a efetivação da política de Governo Eletrônico permitiu a interação entre outras iniciativas e projetos, que já estavam sendo desenvolvidas, entre elas o programa "Sociedade da Informação (SocInfo)" (BRASIL, 2002). Esse programa teve como objetivo promover ações que desenvolvessem a utilização das TIC, de forma a favorecer, por meio da tecnologia, a inclusão social da população em uma sociedade inserida na era digital e, ao mesmo tempo, contribuir para que a economia do país tivesse a capacidade de ser competitiva em nível mundial (TAKAHASHI, 2000).

O SocInfo desenvolveu o programa baseado em sete linhas de ações a serem implementadas e compartilhando as responsabilidades dessa implementação entre três setores, a saber: i) governo; ii) iniciativa privada e iii) sociedade civil. Segundo Takahashi (2000, p. 11), "o compartilhamento das responsabilidades entre governantes, organizações privadas e a sociedade civil é modelo básico de apoio à sociedade da informação". As linhas de ação apresentadas pelo programa foram: i) mercado, trabalho e oportunidades; ii) universalização de serviços para a cidadania;

iii) educação na sociedade da informação; iv) conteúdos e identidade cultural; v) governo ao alcance de todos; vi) pesquisa e desenvolvimento de tecnologias-chave e aplicações e, vii) infraestrutura avançada e novos serviços.

Analisando as linhas de ação do SocInfo, Prado (2009, 72) argumentou que o foco principal do programa estava centrado “na promoção do comércio eletrônico e na consequente integração entre governo, mercado e fornecedores”, porém as ações para o desenvolvimento do governo eletrônico, de responsabilidade do GTTI, se deteve especificamente em três linhas de ação: i) universalização do acesso do cidadão aos serviços prestados pelo Governo, ii) a integração entre os sistemas, redes e bancos de dados da administração pública e iii) a abertura de informações à sociedade, por meio da Internet. De acordo com o CEGE, essas ações, representaram:

> [...] um desdobramento da linha de ação prevista no âmbito da Sociedade da Informação, **com a expectativa de obtenção de ganhos de sinergia**, na medida em que atua principalmente sobre a máquina administrativa do Governo Federal, enquanto esse mantém seu direcionamento amplo para os segmentos empresarial e de pesquisa científica e tecnológica. Por outro lado, o programa Governo Eletrônico se propõe também a utilizar a sua infra-estrutura e recursos para apoiar a universalização do acesso à tecnologia da informação [...] (BRASIL, 2002, p. 8, grifo nosso).

Medeiros e Guimarães (2004, p. 53) reafirmam que as atividades do GTTI estavam em conformidade com as metas do Programa Sociedade da Informação, fazendo com que o GTTI assumisse “um papel de facilitador na busca dos objetivos do SocInfo”. Mantovane (2012, p. 38) corrobora essa afirmação ao dizer que o documento “Proposta de Política de Governo Eletrônico”, desenvolvido pelo GTTI, estava em “sintonia permanente com os objetivos e linhas de ação do Programa Sociedade da Informação”.

O GTTI ressaltou a importância do SocInfo no desenvolvimento do programa de governo eletrônico ao considerar que “ação do governo em tecnologia da informação e comunicação é complementar com o Programa Sociedade da Informação [...] que estabelece normas para a ampliação da competitividade e da produtividade [...]” (BRASIL, 2000b, p. 3-4). Os programas “Governo Eletrônico” e “SocInfo” foram, conjuntamente, fundamentais para os objetivos do governo em adotar uma política nacional que permitisse o desenvolvimento das TIC e facilitasse

o amplo acesso de toda a sociedade aos serviços e benefícios oriundos das TIC, colocando o país no contexto de uma sociedade agora inserida na era digital.

2.2.3 Outras Iniciativas e Críticas

O marco inicial para o desenvolvimento do Programa de Governo Eletrônico pode ser considerado as publicações da “Proposta de Política de Governo Eletrônico para o Poder Executivo Federal”, de responsabilidade do CEGE e o “Livro Verde da Sociedade da Informação”, de responsabilidade do Ministério de Ciência e Tecnologia (MCT), pois como salientado por Medeiros e Guimarães, no Brasil, os projetos de governo eletrônico foram desenvolvidos em duas vertentes de atuação, quais sejam:

> 1) nas diretrizes do Comitê Executivo do Governo Eletrônico, executadas por meio do Programa Governo Eletrônico e outros programas governamentais e 2) em três das sete linhas de ação do Programa SocInfo – “Universalização de Serviços para a Cidadania”, “Governo ao Alcance de Todos” e “Infra-estrutura Avançada e Novos Serviços” (MEDIROS; GUIMARÃES, 2004, p. 54).

A partir dessas iniciativas basilares para o primeiro passo na implementação do governo eletrônico no país, outras normas e orientações são constantemente publicadas no âmbito desse projeto, no intuito de melhorar, facilitar e desenvolver tanto o programa de governo eletrônico, quanto o trabalho dos diversos grupos envolvidos na normatização, execução, controle e monitoramento do referido programa.

Esse estudo não tem como escopo descrever todas as ações desenvolvidas, normas, leis ou decretos para a implementação do Programa de Governo Eletrônico no Brasil. Apresentaremos, nesse tópico, de forma sucinta, algumas importantes etapas adotadas ao longo do processo de implementação do programa, bem como algumas críticas realizadas por autores e organizações. O Quadro 2 apresenta essas etapas:

Quadro 2 - Etapas do desenvolvimento do Programa Governo Eletrônico no Brasil

	FATOR/MARCO	INFLUÊNCIAS DO PROGRAMA
GOVERNO FERNANDO HENRIQUE (1995 - 2002)	Uso das TIC nos processos de reforma do Estado	A possibilidade de uso das TICs no auxílio às iniciativas de reforma coloca a questão da criação do programa de governo eletrônico como parte das ações do governo.
	Criação do GTTI	Criado com a finalidade de examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação, forneceu as bases para a criação do programa.
	Criação do Programa de Governo Eletrônico	A partir dos resultados dos trabalhos do GTTI, foi lançado um documento contendo a política de governo eletrônico, que iria estruturar a criação do programa e o estabelecimento de sua estrutura institucional.
	Livro Verde Sociedade da Informação	Livro que contemplava as metas de implementação do programa Sociedade da Informação com o objetivo de desenvolver aspectos como: ampliação do acesso, meios de conectividade, formação de recursos humanos, incentivo à pesquisa e desenvolvimento, comércio eletrônico, desenvolvimento de novas aplicações.
	Criação do CEGE	Criado com o objetivo de formular políticas, estabelecer diretrizes, coordenar e articular as ações de implantação do Governo Eletrônico, marcou o compromisso do governo com o desenvolvimento do programa.
	Suporte institucional do CEGE	A força política e determinação de Pedro Parente na condução das atividades do CEGE são decisivas na superação dos obstáculos iniciais do programa. Seu suporte na coordenação do CEGE marca a consolidação do programa na agenda governamental.
	Crise energética	A crise energética brasileira ocasiona o deslocamento de Pedro Parente para a Câmara de Gestão da Crise. Isso causa a perda de destaque do programa no governo e a redução no ritmo das iniciativas. O programa deixa de ter prioridade.
	Eleições presidenciais	Como resultado do fortalecimento da candidatura de Lula, a prioridade governamental vincula-se aos programas de mais impacto perante a opinião pública e, após a derrota, à entrega de um governo com estabilidade macro-econômica. Com isso, ações de longo prazo, como o governo eletrônico, perdem prioridade.
GOVERNO LULA (2003 - 2010)	Transição de governo	A descontinuidade de ações durante o período de transição afeta o programa. Surgem problemas de articulação institucional entre a SLTI e os demais Ministérios.
	SLTI assume a coordenação informal do CEGE	A SLTI passa a ocupar o vazio deixado pela falta de reuniões do CEGE, assumindo a coordenação —de fatoll dos trabalhos do CEGE
	Criação dos Comitês Técnicos	Os CTs são criados para dar suporte técnico ao CEGE. Tornam-se as instâncias de discussão das políticas e de integração com os demais órgãos da APF.
	Definição das novas prioridades do programa	As novas prioridades colocam a questão do controle social e da promoção da cidadania como fios condutores do programa. O programa, todavia, começa a apresentar evidentes sinais de perda de prioridade na agenda governamental.
	Criação do Departamento Governo Eletrônico (DGE)	O DGE é criado para assumir algumas ações do programa, em especial quanto ao monitoramento e avaliação do desenvolvimento de projetos de governo eletrônico.

	e-Ping	Criação da primeira versão dos Padrões de Interoperabilidade que buscou estabelecer condições de interação entre sistemas.
	Criação do Portal de Convênios	Com participação do DGE na sua criação, o Portal de Convênios representa uma das mais importantes ações do programa relacionada à transparência.
	e-Nota	sistema informatizado para emissão de Notas Fiscais Eletrônicas de Serviços, visando a modernização da Gestão Tributária.
GOVERNO DILMA (2011 - 2016)	Licença Pública de Marca	Lançamento da primeira versão da Licença Pública de Marcas (LPM) que tem como objetivo o fortalecimento de desenvolvimento de softwares públicos.
	Lei de Acesso à Informação	Lei que regulamenta o direito constitucional de acesso às informações públicas, onde qualquer pessoa, física ou jurídica, pode requerer informações públicas sem necessidade de apresentar motivos, desde que resguardada as devidas restrições. O acesso passa a ser a regra.
	Portal Brasileiro de Dados Abertos	Local na internet onde será compartilhado dados públicos em formato bruto e aberto, ou seja, sem nenhum tipo de tratamento ou análise.
	Infovia Brasília	Projeto de infraestrutura de rede ótica para fornecer, aos órgãos do Governo Federal situados em Brasília, um conjunto de serviços e funcionalidade visando à redução de custos de comunicação.
	Identidade Digital de Governo (IDG)	Projeto para a padronização dos portais do órgãos públicos federais e alinhamento das informações com o intuito de otimizar a comunicação com o cidadão.
	Suite VLibras	Projeto para o desenvolvimento de um conjunto de ferramentas computacionais de código aberto, responsável por traduzir automaticamente conteúdos digitais (texto, áudio e vídeo) em Língua Brasileira de Sinais (LIBRAS).

Fonte: Adaptado de Prado, Ribeiro e Diniz (2009); Mantovane (2012); e informações do site do governo eletrônico (2016).

As políticas e ações para implementação do governo eletrônico no Brasil foram analisadas criticamente por Mantovane (2012) considerando os governos de Fernando Henrique Cardoso (FHC) (1995-2002) e Luis Inácio Lula da Silva – (Lula) (2003-2010). O autor ressaltou que na gestão do presidente FHC, e em função do envolvimento do ministro Pedro Parente, o governo eletrônico teve grande destaque na agenda governamental, o que possibilitou a criação de uma ampla estrutura para o desenvolvimento das políticas desse programa. Prado (2009, p. 160) ressalta que no governo FHC o programa de governo eletrônico:

> [...] esteve claramente direcionado a ações que visassem a melhoria dos processos internos do governo, indicando que o conceito adotado para direcionamento do programa se aproximou da definição de governo eletrônico como relacionado ao uso das TICs pelo governo para melhoria da gestão.

Com a mudança de governo em 2003, o programa de governo eletrônico:

> [...] demonstrou um refluxo nas atividades até então desenvolvidas, ganhando novas configurações a partir de 2004. Isso indica uma ruptura com alguns preceitos cultivados durante o governo FHC e a mudança de foco da política. Na gestão do governo Lula, [...] buscou-se uma maior ênfase nos temas sociais e na defesa de adoção de software livre e de código aberto [...] (MANTOVANE, 2012, p. 52).

Prado (2009) argumentou que a falta de uma equipe de transição entre os governos FHC e Lula, trouxe descontinuidade às atividades que eram conduzidas pelo CEGE e que somente em 2004, com a criação do Departamento de Governo Eletrônico (DGE), as atividades foram retomadas. Para o autor, o programa de governo eletrônico não teve espaço destacado na agenda do governo Lula, mas as atribuições definidas para o programa, à época do governo Lula, indicavam que:

> [...] o conceito adotado na atual gestão se aproxima da definição de governança eletrônica expressa pelas organizações supranacionais, como a ONU e a OECD, já que a ênfase tem recaído com mais intensidade no uso das TICs como instrumentos para a melhoria da relação entre governo e sociedade (PRADO, 2009, p. 160).

No tocante ao governo Dilma, talvez a iniciativa mais contundente em relação ao programa de governo eletrônico tenha sido a criação, em 2011, da lei nº. 12.527, conhecida como Lei Acesso à Informação. Essa lei veio regulamentar o texto já disposto no art. 5º, incisos XIV e XXXIII, da Constituição, na qual é assegurado o acesso às informações públicas a todos os interessados. Raminelli, Rodegheri e Oliveira (2014, p.144) argumentam que a criação dessa lei se insere no contexto de:

> [...] modelo de governo eletrônico no país e das diretrizes internacionais de uma transparência governamental acerca das ações tomadas pelos governos na Administração Pública, bem como em consonância com as previsões constitucionais brasileiras de acesso à informação [...]

Outra mudança adotada pelo governo Dilma foi a extinção do Comitê Executivo do Governo Eletrônico e dos Comitês Técnicos do CEGE, bastante atuantes no início da implantação do Programa de Governo Eletrônico. Os decretos que os criaram foram revogados pelo Decreto Presidencial nº. 8.638, de 15 de janeiro de 2016, que instituiu a “Política de Governança Digital” para os órgãos e entidades da administração publica federal. Esse decreto também definiu que fosse editado o documento “Estratégia de Governança Digital” (EGD) com a definição dos

objetivos estratégicos, as metas, os indicadores e as iniciativas da Política de Governança Digital.

Outro decreto revogado foi o da criação do Departamento de Governo Eletrônico, sendo agora substituído pelo Departamento de Governança Digital conforme o Decreto Presidencial nº. 8.818 de 21 de julho de 2016.

A Política de Governança Digital é considerada, pelo Governo Federal, um novo estágio do governo eletrônico no Brasil, pois esse programa necessitava uma reestruturação das ações alinhada aos avanços da tecnologia e das demandas da sociedade. A Política de Governança Digital baseia-se na ideia do cidadão deixar de ser apenas um consumidor de informações e serviços para se tornar "partícipe da construção de políticas públicas que já nascem em plataformas digitais, abrangendo não só a internet, mas também outros canais como a TV Digital" (BRASIL, 2016c, p. 10).

2.3 SEGURANÇA DA INFORMAÇÃO

Vários campos científicos utilizam o conceito de informação dentro de seu próprio contexto e de acordo com determinados fenômenos específicos, o que o torna um conceito interdisciplinar suscitando em diversas teorias e abordagens com diferentes perspectivas (CAPURRO; HJØRLAND, 2003). Nesse estudo, o conceito de informação que nos interessa é o contido na norma 27002:2013 da Associação Brasileira de Normas Técnicas (ABNT) que considera a informação como um ativo e "[...] como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos." (ABNT – NBR 27002, 2013, p. x).

A informação pode estar contida em diversos suportes/mídias. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Independente de qual seja a maneira na qual é apresentada ou a forma de compartilhamento/armazenamento da informação, recomenda-se a sua adequada proteção com vista a assegurar a competitividade, a lucratividade e a imagem da organização junto ao mercado (ABNT – NBR 27002, 2013).

Conforme Dantas (2011, p. 9), a informação, devido à sua importância, tem sido imprescindível “na manutenção dos negócios e realização de novos empreendimentos entre pessoas, empresas, povos, nações e blocos econômicos”.

A importância da informação também é destacada pelo Tribunal de Contas da União (BRASIL, 2012, p. 10) que considera a informação “um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico”. Também ressaltada pela Secretaria de Assuntos Estratégicos (SAE) da Presidência da República, na atual Era do Conhecimento a informação:

> foi alçada à categoria de ativo estratégico para organizações e Estados-Nação, conferindo àqueles que a detém e dela se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais (CARVALHO, 2011, p. 15).

Pode-se inferir que a informação tem a capacidade de explorar oportunidades, reduzir incertezas, melhorar a relação entre os diversos interessados e contribuir para o desenvolvimento econômico tanto de empresas quanto do país, e, nesse sentido, é necessário que se busque maneiras de garantir sua segurança contra qualquer tipo de ameaça.

A Norma 27000:2014 da *International Standards Organization* (ISO) define segurança da informação como a proteção contra qualquer tipo de ameaça que possa comprometer a confidencialidade, integridade e/ou a disponibilidade da informação. A Instrução Normativa nº. 1 de 13 de junho de 2008, emitida pelo Gabinete de Segurança Institucional da Presidência da República adiciona à segurança da informação o termo “comunicações” e considera que Segurança da Informação e Comunicações são “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações” (BRASIL, 2008a, p. 2).

Uma definição mais ampla é dada pelo Decreto Presidencial nº. 3.505 de 13 de junho de 2000, que conceitua segurança da informação como a:

> [...] proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações

> e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (BRASIL, 2000c).

Como já explicitado, a informação é considerada um ativo, e como tal, possui valor. O valor de uma informação decorre diretamente de conseguir garantir três características fundamentais da informação: i) a integridade; ii) a disponibilidade e iii) a confidencialidade (WHITMAN; MATTORD, 2011; DANTAS, 2011). Ainda segundo os autores, essas características formam os princípios da segurança da informação.

A importância das características que formam os princípios da segurança da informação é ressaltada pela ABNT 27002 (2013, p. 19), ao afirmar que o nível de proteção da informação pode ser avaliado “por meio da análise da confidencialidade, integridade e disponibilidade [...]”. Conforme Dantas (2011), qualquer ação que comprometa qualquer um dos três princípios é um atentado contra a segurança da informação.

2.3.1 Integridade

A definição técnica da ISO 27000 (2014) conceitua integridade como a propriedade de proteger a exatidão e a plenitude dos ativos. Em outras palavras o TCU explicita que integridade consiste na fidedignidade de informações como também:

> Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital (BRASIL, 2012, p. 9).

A integridade das informações é fundamental aos sistemas de informação, pois a informação não possuirá nenhum valor se os usuários não puderem verificar sua integridade (WHITMAN; MATTORD, 2011).

2.3.2 Disponibilidade

A disponibilidade é propriedade de que “a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou

entidade” (BRASIL, 2008a, p. 2). A disponibilidade de uma informação é a garantia de que ela esteja disponível sempre que necessário às pessoas e aos processos autorizados e preservar sua disponibilidade “pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito” (BRASIL, 2012, p. 10).

2.3.3 Confidencialidade

A informação tem confidencialidade quando é protegida contra divulgação ou exposição a pessoas ou sistemas não autorizados. Confidencialidade garante que apenas aqueles com os direitos e privilégios de acesso à informação são capazes de fazê-lo (WHITMAN; MATTORD, 2011). O TCU considera que manter a confidencialidade “pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento” (BRASIL, 2012, p. 9).

Além dessas três propriedades básicas que asseguram a informação, a ISO 27000 (2013) também destacou que outras propriedades poderiam ser envolvidas a fim de possibilitar a segurança da informação, a saber: i) autenticidade; ii) responsabilidade; iii) não repúdio e iv) confiabilidade. Conforme explicitado por Dantas (2011, p. 15):

> [...] a autenticidade do emissor é a garantia de que quem se apresenta como remetente é realmente quem diz ser. A confiabilidade é a garantia de que a informação está completa e igual à sua forma original quando do envio pelo remetente, e expressa uma verdade. O não repúdio é a garantia de que o emissor ou receptor não tem como alegar que a comunicação não ocorreu, e a responsabilidade diz respeito aos deveres e proibições entre remetente e destinatário.

Observa-se que, com o desenvolvimento constante dos meios e tecnologias de comunicação, vem sendo necessário, além dos três pilares básicos para a segurança da informação, que outras premissas sejam discutidas e incorporadas ao tema a fim de assegurar sua proteção contra qualquer tipo de ameaça que ponha em risco o seu valor. Em função do aumento da interconectividade entre redes públicas e privadas, a informação é submetida a uma grande variedade, sempre crescente, de ameaças, entre elas: fraudes eletrônicas, espionagem, sabotagem,

vandalismo, fogo, inundação, blackouts, códigos maliciosos, hackers, ataques de DDoS, entre outras.

2.4 AMEAÇAS, VULNERABILIDADES E ATAQUES

O principal objetivo da segurança da informação é a garantia de que os sistemas de informação e seus conteúdos não sofram alterações não permitidas. No entanto, novas vulnerabilidades são descobertas a todo o momento, constituindo um ambiente propício a ameaças e consequentemente à ataques. Esse tópico irá descrever as ameaças, vulnerabilidades e ataques a que estão sujeitos os sistemas de informação eletrônica.

2.4.1 Ameaças

De acordo com a ISO 27000 (2014, p. 11), ameaça é “uma causa potencial de incidente não desejado, podendo resultar em danos para um sistema ou organização”. No contexto de segurança da informação, uma ameaça poderá ser um objeto, pessoa, ou qualquer coisa que represente um perigo contínuo para um ativo (WHITMAN; MATTORD, 2011).

Foi apresentado por Whitman e Mattord (2011, p. 44), um quadro com 14 categorias gerais de ameaças que representam perigos presentes para as pessoas de uma organização, conforme Quadro 3.

Quadro 3 - Categorias de ameaças

	CATEGORIA DE AMEAÇAS	**EXEMPLOS**
1	Comprometimento da Propriedade Intelectual	Pirataria, Violação de direitos autorais
2	Ataques de Software	Vírus, Worms, Macros, DDoS
3	Desvios na qualidade do serviço	Problemas na prestação dos serviços de Provedores de Internet
4	Espionagem ou violação	Acesso não autorizado e/ou roubo de dados
5	Forças da natureza	Fogo, inundação, terremoto, relâmpago
6	Erro ou falha humana	Acidentes, erros de empregados
7	Chantagem	Blackmail, ameaça de divulgação de informações
8	Perda, inadequação ou incompletude dos dados	Perda de acesso aos sistemas de informação devido ao disco rígido apresentar problemas e não haver um disco apropriado de backup de recuperação

9	Perda, inadequação ou controles incompletos	Rede comprometida, pois não há nenhum firewall assegurando o controle
10	Sabotagem ou vandalismo	Destruição de sistemas ou informações
11	Roubo	Apropriação ilegal de equipamentos ou informações
12	Falhas e/ou erros técnicos em hardwares	Falhas de equipamento
13	Falhas e/ou erros de software	Bugs, erros de código, lacunas desconhecidas
14	Obsolescência tecnológica	Tecnologias antiquadas ou obsoletas

Fonte: Whitman e Mattord (2011, p. 44).

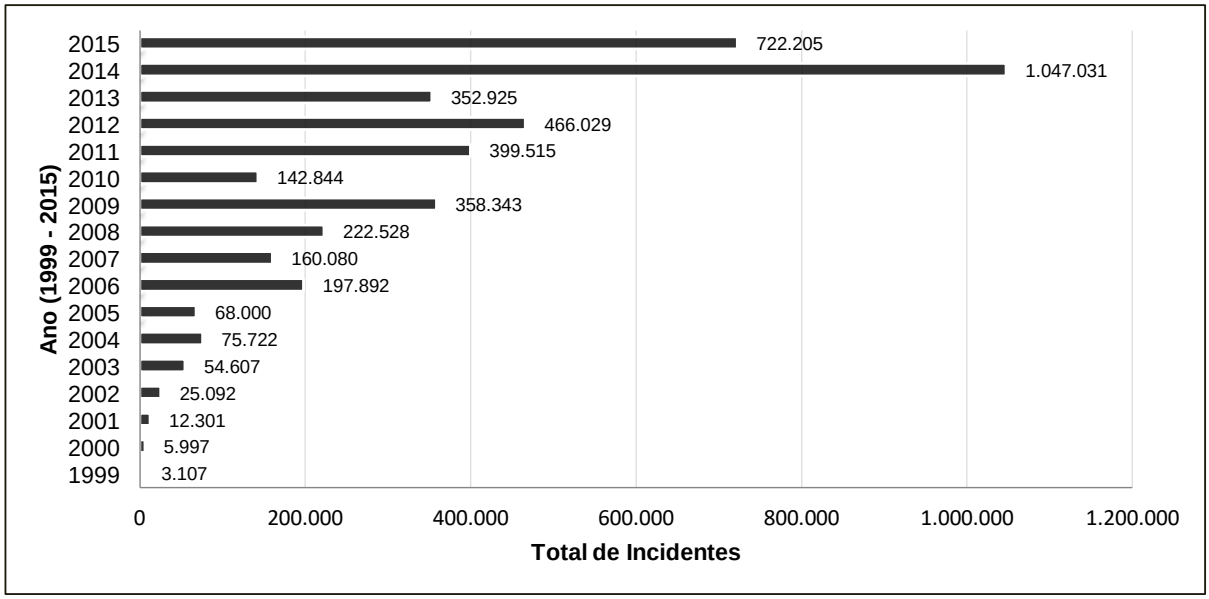
Verifica-se, pelo Quadro 3, um grande número de ameaças com possibilidade de colocar em risco os ativos de uma organização e a continuidade de suas operações. Ainda segundo Whitman e Mattord (2011), cada organização deve priorizar as ameaças que enfrenta, tendo em vista a estratégia organizacional de gestão de risco, adequando aos níveis de exposição ao risco em que seus ativos operam.

O Quadro 3 foi evidenciado apenas para exemplificar os diversos tipos ameaças às organizações e/ou ativos de informação, mas como já exposto, nosso intuito é identificar as possíveis ameaças eletrônicas a que estão expostos os portais de governo eletrônico do Brasil.

Como ressaltado por Silva (2011, p. 130), “a sociedade está cada vez mais dependente – talvez absolutamente – das tecnologias, as quais os próprios adversários podem se utilizar para atacar”. Em um mundo cada vez mais interconectado, as ameaças eletrônicas se propagam de maneira exponencial, tendo em conta o rápido avanço da internet, onde é possível identificar essa expansão de ameaças pelo aumento no número de incidentes registrados.

No Brasil, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é o responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet Brasileira e define incidente de segurança como “qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores” (CERT.br, 2012, p. 50). O CERT.br monitora e disponibiliza em seu site, estatísticas de incidentes ocorridos no Brasil. Como exemplo, o Gráfico 1 apresenta o total de incidentes anuais que foram reportados ao CERT.br relativos aos anos de 1999 à 2015.

Gráfico 1 - Total de incidentes reportados ao CERT.br por ano



Fonte: Adaptado do site do CERT.br (2016 - estatísticas).

Esses incidentes são ligados a vários tipos de ameaças/ataques que comprometem os ativos de informação ameaçando sua segurança e a continuidade das atividades de uma organização. Detalhando o ano de 2014 e 2015 por quantidade e tipo de ataque, verificamos a seguinte composição dos tipos de ataques às redes de computadores, conforme a Tabela 1.

Tabela 1 - Quantidade e tipos de ataques no ano de 2015

Tipo de ataque	2014	%	2015	%	Δ %
Worm	42.191	4,0%	47.722	6,6%	13,1%
DoS	223.935	21,4%	25.360	3,5%	-88,7%
Invasão	6.509	0,6%	2.457	0,3%	-62,3%
Web	28.808	2,8%	65.647	9,1%	127,9%
Scan	263.659	25,2%	391.223	54,2%	48,4%
Fraude	467.621	44,7%	168.775	23,4%	-63,9%
Outros	14.308	1,4%	21.021	2,9%	46,9%
Total	**1.047.031**	**100,0%**	**722.205**	**100,0%**	

Fonte: Adaptado do site do CERT.br (2016 - estatísticas).

Destaque para o aumento de 127,9% das notificações de ataques à servidores *Web* comparando o ano de 2015 em relação ao ano de 2014. Conforme o Núcleo de Informação e Coordenação do Ponto BR (NIC.br, 2016), os atacantes

exploram vulnerabilidades em aplicações *Web* para hospedar, nesses sítios, páginas falsas de instituições financeiras, Cavalos de Troia (usados para furtar informações e credenciais), ferramentas utilizadas em ataques a outros servidores *Web* e *scripts* para envio de *spam* ou *scam*.

A Administração Pública Federal (APF) também possui um centro próprio com propósito de notificação, análise e tratamento de incidentes chamado de Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.Gov). A finalidade desse centro é o atendimento aos incidentes em redes de computadores da Administração Pública Federal, Estadual e Municipal. A Tabela 2 mostra os incidentes relatados ao CTIR.Gov no ano de 2015 e no 1º semestre de 2016.

Pela Tabela 2 observa-se que dos incidentes relatados no ano de 2015, 65% deles estão distribuídos entre quatro ameaças: i) Abuso de Sítio (24%); ii) Indisponibilidade de Sítio (10%); Página Falsa (16%); *Phishing Scam* (15%). Quando comparamos o 1º semestre de 2016 em relação ao 1º semestre de 2015, verifica-se que houve um significativo aumento dos incidentes em três categorias: i) Indisponibilidade de Sítio (55%); ii) Scaneamento de Vulnerabilidades (109%) e iii) Vazamento de Informação (1.172%).

Tabela 2 - Quantidade de incidentes por categoria na APF

	2015				**2016**		
Categoria	**1º sem**	**2º sem**	**Total**	**%**	**1º sem**	**%**	**Δ % (1º e 2º sem)**
Abuso de Sítio	1.334	1.010	2.344	24%	1.166	22%	-13%
Abuso de SMTP	307	389	696	7%	389	7%	27%
Análise de Malware	190	196	386	4%	216	4%	14%
Botnets	98	28	126	1%	68	1%	-31%
DNS Malicioso	256	3	259	3%	3	0%	-99%
DNS Recursivo	8	8	16	0%	2	0%	-75%
Geral	24	21	45	0%	20	0%	-17%
Hospedagem de Artefatos	23	37	60	1%	23	0%	0%
Hospedagem de Malware	359	178	537	6%	169	3%	-53%
Indisponibilidade de Sítio	507	447	954	10%	788	15%	55%
Página Falsa	922	662	1.584	16%	766	15%	-17%
Phishing Scam	650	791	1.441	15%	566	11%	-13%
Redirecionamento de Malware	219	188	407	4%	211	4%	-4%

Scaneamento de Vulnerabilidades	119	239	358	4%	249	5%	109%
Trasnferência de Zona DNS	-	96	96	1%	-	0%	-
Vazamento de Informação	47	286	333	3%	598	11%	1172%
Violação de Direitos Autorais	5	-	5	0%	3	0%	-40%
Total	**5.068**	**4.579**	**9.647**	**100%**	**5.237**	**100%**	

Fonte: Adaptado do site do CTIR Gov (2016 - estatísticas).

Esses números, apesar de não representarem a totalidade dos incidentes de segurança, podem ser considerados como uma amostra das principais ameaças, e servir como base para orientar ações proativas e investimentos necessários ao fortalecimento da Segurança das Redes de Governo (CIRT.Gov, 2015).

2.4.2 Vulnerabilidades

De acordo com a norma ISO 27000 (2014, p. 12), vulnerabilidade é a "fragilidade em um ativo, ou processo, que pode ser explorada por uma ou mais ameaças". Outras definições definem vulnerabilidade como uma fragilidade em um processo ou programa que torna o sistema suscetível a um ataque ou dano (BORDER, 2006); ou ainda, um conjunto de condições dentro de um produto que, em decorrência de erro no projeto ou má implementação, pode ser explorada por um atacante e resultar em uma violação de segurança (ALEXANDER; GILES, 2006; CERT.br, 2012).

Merkow (2006) considera que a vulnerabilidade pode ser resultado de uma falha na automação do sistema de segurança, nos controles administrativos, *layout* físico e controles internos, podendo ser explorada por uma ameaça para obter acesso não autorizado a informações ou interromper a continuidade das atividades.

Observa-se, das definições acima, que as vulnerabilidades estão diretamente relacionadas às fragilidades existentes em um ativo, podendo estar presentes em procedimentos automatizados, sistemas de segurança, controles administrativos, *layout* físico, controles internos, equipamentos, funcionários sem treinamento, funcionários desmotivados, falta de uma política de segurança, etc. Dada a extensa lista de possibilidades, a ABNT 27005 (2008, p. 42-45) fornece exemplos de vulnerabilidades em diversas áreas de segurança classificando-as como: i) de *hardware*; ii) de *software*; iii) de Rede; iv) Recursos Humanos; v) Local ou

Instalações e vi) Organização. Alguns exemplos de vulnerabilidades descritos pela ABNT 27005:2008 podem ser vistos no Quadro 4.

Quadro 4 - Exemplos de Vulnerabilidades

Tipos	**Exemplos de vulnerabilidades**
Hardware	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira ou sujeira
	Sensibilidade a variações de voltagem
	Armazenamento não protegido
Software	Falhas conhecidas no *software*
	Não execução do "*logout*" ao se deixar uma estação de trabalho
	Atribuição errônea de direitos de acesso
	Interface de usuário complexa
Rede	Inexistência de mecanismos de autenticação e identificação
	Gerenciamento mal feito de senhas
	Especificações confusas o incompletas para os desenvolvedores
	Inexistência de cópias de segurança
Recursos Humanos	Procedimentos de recrutamento inadequados
	Treinamento insuficiente em segurança
	Uso incorreto de *software* e *hardware*
	Falta de conscientização em segurança
Local ou Instalações	Localização em área suscetível a inundações
	Fornecimento de energia instável
	Inexistência de mecanismos de proteção física no prédio portas e janelas
Organização	Processo disciplinar no caso de incidentes de segurança inexistente
	Ausência de registros de auditoria (*logs*)
	Política de uso de e-mail inexistente

Fonte: Adaptado da ABNT 27005 (2011).

As ameaças também estão diretamente relacionadas às vulnerabilidades, mas, é preciso ressaltar que uma ameaça não pode ocorrer sem a existência de uma vulnerabilidade, ou seja, caso não haja vulnerabilidades no ativo, as ameaças não terão nenhum impacto sobre ele. A essa afirmação, Alexander e Giles (2006) destacam que as estratégias de segurança definem as proteções contra ameaças e não vulnerabilidades.

Whitman e Mattord (2011) consideram que sempre haverá vulnerabilidades, conhecidas ou não, e a segurança de seus ativos de informação poderá estar

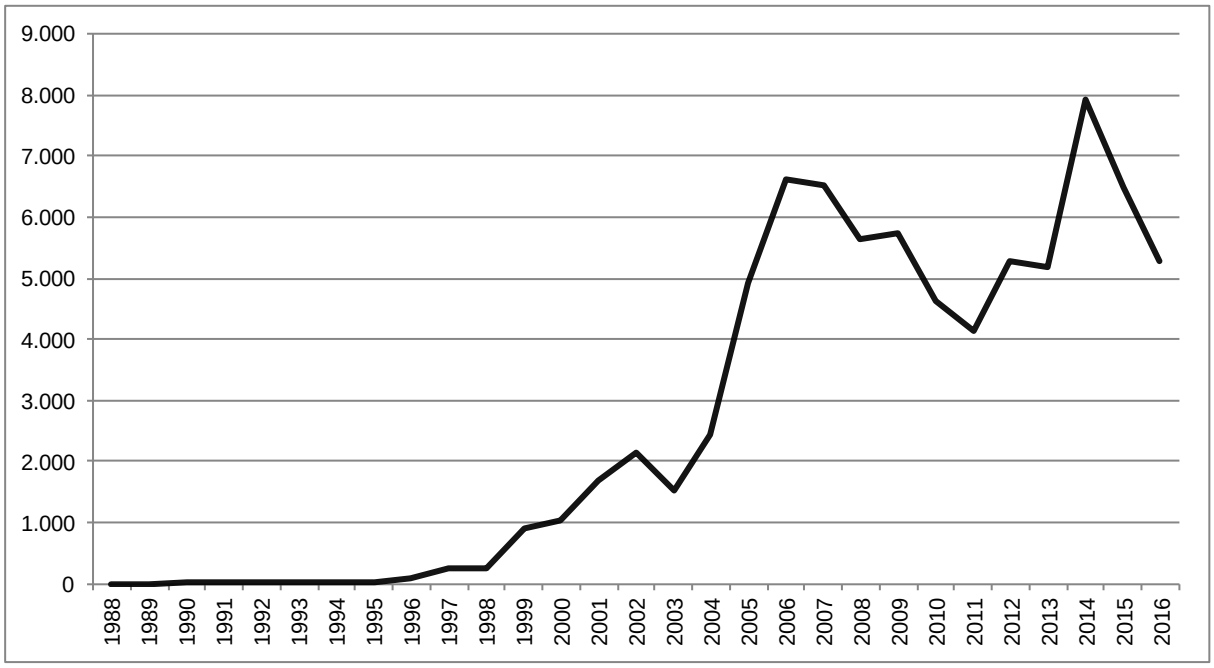
constantemente comprometida, devendo então ser mantido um controle da segurança da informação adotando uma verificação constante das ameaças, vulnerabilidades, ativos e vítimas potenciais, a fim de que a organização reduza a sua exposição aos ataques e tenha uma capacidade rápida de resposta aos possíveis incidentes.

Em um mundo cada vez mais interconectado pela rede mundial de computadores, as ameaças *online* tem se expandido com enorme velocidade, comprometendo a segurança da informação pela exploração das vulnerabilidades dos ativos de informação. Para a *Australian Cyber Security Centre Threat* (ACSC) as ameaças cibernéticas (*cyber threat*) são “inegáveis, implacáveis e continuam a crescer” e, além disso, “se uma organização está conectada à internet, ela é vulnerável. Os incidentes conhecidos pelo público são apenas a ponta do iceberg” (ACSC, 2015, p. 2, tradução nossa). Pode-se inferir que vulnerabilidades e ataques à aplicações *Web* estão diretamente relacionados.

A Symantec, em seu *Internet Security Threat Report* (2016), relata que no ano de 2015 mais de um milhão de pessoas sofreram ataques pela *Web,* com um agravante, pois estas acreditavam estarem seguras ao acessarem sites autênticos. Neste relatório a Symantec ressalta que mais de 75% dos sites autênticos possuem vulnerabilidades não corrigidas, e 15% dos sites autênticos possuem vulnerabilidades consideradas críticas, significando não ser necessário um grande esforço do atacante para obter acesso e comprometer a segurança.

A *National Vulnerability Database* (NVD), patrocinada pelo governo dos Estados Unidos, é um repositório de dados sobre as vulnerabilidades identificadas em softwares. De acordo com o NVD, de 1998 à agosto de 2016, mais de 78.000 vulnerabilidades foram identificadas e sua evolução pode ser vista no Gráfico 2.

Gráfico 2 - Número de vulnerabilidades encontradas (1998 – 2016)



Fonte: Adaptado do site do NVD (2016 - statistics).

Ameaças e vulnerabilidades tem sido o problema de vários governos que enfrentam uma expansão das ameaças *online* tendo como consequência o aumento dos incidentes de segurança e os custos para resolvê-los. O *Government Accountability Office* (GAO, 2015), que é a agência de prestação de contas do governo dos Estados Unidos, relatou que em menos de uma década houve um forte aumento (1.120%) nos incidentes de segurança da informação, relatado por agências federais dos Estados Unidos, passando de 5.503 incidentes por ano em 2006 para 67.168 incidentes em 2014. O relatório da ACSC (2015) destacou que, em 2014, mais de 11.000 incidentes de segurança cibernética afetaram empresas australianas, sendo que, desses incidentes, 153 envolveram sistemas de interesse nacional e de infraestrutura (energia, serviços públicos).

Em 2015, o *Ponemon Institute* analisou o custo de ataques cibernéticos no Brasil. Especificamente no setor público brasileiro, o custo anual estimado de ataques cibernéticos foi de aproximadamente R$ 12,4 milhões e a média anual do custo de todas as indústrias componentes do estudo foi de aproximadamente R$ 15 milhões. O *Ponemon Institute* (2015a, p. 1) ressalta que o “Brasil é o segundo maior gerador de crimes cibernéticos do mundo, tanto como origem, quanto como alvo de ataques *online*”.

Um estudo global do custo dos crimes cibernéticos foi realizado em 2014 pelo *Center for Strategic and International Studies* (CSIS, 2014), no qual estimaram que os crimes cibernéticos são responsáveis por perdas anuais à economia global, no montante de mais de US$ 400 bilhões. O CSIS acredita que esse número esteja subestimado, pois ressaltam que a maioria dos crimes virtuais não são notificados. Em outro estudo, esse realizado pela *Juniper Research* (2015), estima-se que o custo de crimes cibernéticos alcançará, em 2019, o valor de US$ 2,1 trilhões em todo o mundo.

Os atacantes virtuais possuem grande vantagem, pois precisam encontrar apenas uma vulnerabilidade, muitas vezes já conhecida, e explorá-la, enquanto a organização deve se defender a partir de milhões de ataques iminentes contra todos os seus ativos e vulnerabilidades (WHITMAN; MATTORD, 2011), que não mais se restringem ao espaço físico, pois com a disseminação das redes eletrônicas de informação e a integração entre diferentes infraestruturas mostra que a interdependência cada vez maior “[...] da área de TIC acarreta exposição e vulnerabilidades e um conjunto cada vez maior de oportunidades para exploração por parte dos inescrupulosos [...]” (SILVA, 2011, p. 141).

2.4.3 Ataques

Qualquer investida mal-intencionada, realizada por indivíduos ou organizações, contra sistemas de informação computadorizados, infraestruturas, redes de computadores e/ou computadores pessoais, será considerado um ataque cibernético (PONEMON INSTITUTE, 2015a). As notícias destacadas a seguir são uma amostra das vulnerabilidades existentes em sistemas de informação que são exploradas diariamente por atacantes mal intencionados com os mais diversos objetivos, permitindo, a eles, o controle ou ainda o comprometimento dos sistemas, causando prejuízo a organizações públicas, privadas e pessoas.

Em 2014, a BBC Brasil noticiou que:

> Um grupo de *hackers* chamado *CyberVor*, da Rússia, roubou 1,2 bilhão de senhas e nomes de usuários de mais de 500 milhões de endereços de e-mail, segundo a *Hold Security*, uma companhia americana especialista em descobrir falhas em sistemas de segurança (BBC BRASIL, 2014).

Ainda sobre invasão a *Itsecuritynews.Info* (2016, tradução nossa) publicou as seguintes notícias:

> *Hackers* estão coletando dados de cartões de pagamento, utilizados em lojas Magento, escondendo os dados roubados dentro de imagens JPG. Os pesquisadores dizem que os atacantes estão incorporando códigos maliciosos em sites mal configurados, da Magento, que esconde os dados roubados de cartões de pagamento em imagens.
>
> *Hacker* indonésio vai da desconfiguração (*deface*) de *websites* para a instalação de *Ransomware*. O atacante por entender que a desconfiguração de sites é um desperdício de tempo e, do ponto de vista financeiro, insatisfatório, passou a escrever sua própria *Ransomware* baseada em PHP, instalando nos sites desconfigurados por ele, pedindo às vítimas um valor de resgate para liberar o acesso ao site infectado.

Por meio da Internet, sites, grupos e agências governamentais alertam sobre as vulnerabilidades encontradas nas diversas estruturas de informação que permitem a exploração e a possibilidade de catástrofes geradas por ataques cibernéticos.

Conforme a Symantech (2016), experientes grupos de atacantes continuam a lucrar com falhas previamente desconhecidas (*zero-day vulnerability*) nos navegadores. O crescente número de ataques *online,* resultando em violações de segurança, ocasionou o aumento do orçamento destinado à segurança da informação de Governos, Corporações e Indivíduos (VAN DER MEULEN; JO; SOESANTO, 2015).

A norma ISO 27000 (2014, p. 1, tradução nossa) define ataque como “a tentativa de destruir, expor, alterar, inutilizar, roubar, ganhar acesso não autorizado ou fazer uso não autorizado de um ativo”. Um ataque é uma ação que se aproveita de uma vulnerabilidade para comprometer ou controlar um sistema (WHITMAN; MATTORD, 2011), ou ainda, uma ação executada, por um agente de ameaça, para adquirir privilégios do sistema (CHOO, 2011).

O *Ponemon Institute* (2015a, p. 2, tradução nossa) define de forma mais abrangente o conceito e denomina ataque cibernético como:

> [...] qualquer tipo de manobra ofensiva empregada por indivíduos ou organizações que tenham como alvo os sistemas eletrônicos de informação, infraestrutura, redes de computadores ou computadores pessoais, por meio de ações mal intencionadas, normalmente originárias de uma fonte anônima que, ao invadir sistemas vulneráveis, rouba, altera ou destrói um alvo específico (PONEMON INSTITUTE, 2015a, p. 2, tradução nossa).

Verifica-se que as vulnerabilidades existentes nos ativos eletrônicos de informação geram um ambiente propício para a realização de ataques virtuais. De acordo com o GAO (2009), os ataques virtuais podem ser do tipo direcionado e não direcionado. Um ataque virtual direcionado ocorre quando realizado por grupos organizados ou atacantes individuais a um sistema específico ou infraestrutura crítica (telecomunicações, energia) constituída em uma rede (*Internet*). Um ataque virtual não direcionado ocorre quando não existe um alvo específico para o ataque, como, por exemplo, a liberação de códigos maliciosos (vírus, *worm*) na Internet onde qualquer pessoa ou organização pode ser atingida.

O número de ataques virtuais contra governos e organizações comerciais continua a crescer em frequência e gravidade (PONEMON INSTITUTE, 2015b) e mostram uma tendência no aumento de ataques cada vez mais sofisticados e prejudiciais (CHOO, 2011; ACSC, 2015).

O relatório publicado pela *European Union Agency For Network And Information Security* (ENISA) com o panorama das principais ameaças cibernéticas encontradas no ano de 2015 listou dezesseis ameaças que podem ser usadas por atacantes. Abaixo, exemplo de alguns (poucos) tipos de ataques utilizados para a exploração ou controle de sistemas e que causam prejuízos às organizações, tais como:

MALWARE: termo usado para se referir a diversos tipos de *softwares* deliberadamente maliciosos e escritos com o propósito de causar destruição, danos ou roubo de informação de seu alvo. Alguns dos tipos mais comuns de *malware* são vírus, *trojans* e *worms* (SLADE, 2006).

WEB APPLICATION ATTACKS: consistem em injetar, em servidores vulneráveis, códigos maliciosos que comprometam os servidores web onde se encontra a aplicação com o objetivo de alterar o conteúdo do site ou violar a informação (ENISA, 2016a). Alguns tipos de ataques em aplicações *web*, são: i) *Spoofing*; ii) *Repudiation*; iii) *Information Disclosure* e iv) *Denial of Service*.

BOT e BOTNETS: "*Bot* é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente" e *Botnet* é "uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots"* (CERT.br, 2012, p. 26).

DENIAL of SERVICE (DoS): em um ataque *DoS*, o atacante envia um grande número de solicitações de conexão ou de informação a um alvo. Dessa maneira,

com a grande quantidade de solicitações que são feitas, o sistema de destino fica sobrecarregado e não pode responder a pedidos legítimos de serviço. O sistema pode falhar ou simplesmente tornar-se incapaz de realizar funções comuns (WHITMAN; MATTORD, 2011).

As várias possibilidades de ataques cibernéticos causam, agora, bem mais que transtornos, como páginas e serviços *Web* indisponíveis, ou ainda, o roubo de senhas e valores monetários. Outra ameaça crescente no mundo virtual, e motivo de preocupação em governos de todo o mundo, tem sido o uso da *Internet* com propósitos terroristas.

Terrorismo Cibernético pode ser classificado como uma atividade praticada, geralmente, por grupos não estatais que tentam prejudicar pessoas inocentes e, assim, criar um sentimento de medo ou terror entre a população em geral, com o objetivo de defender uma ideologia política (DITTRICH; HIMMA, 2006; ZUCCARO, 2011). “As agressões, em geral, serão dirigidas aos Estados cuja ação ou postura política seja contrária aos interesses ou à visão de mundo daqueles grupos” (ZUCCARO, 2011, p. 61).

As Nações Unidas (UN, 2012) publicaram um relatório sobre a ameaça do terrorismo cibernético, abordando uma visão global dos desafios ao combatê-lo, e propondo diretrizes, políticas, projetos e orientações práticas em aspectos técnicos e legais para combater o uso da *Internet* com propósitos terroristas. Nesse relatório, as Nações Unidas identificaram seis categorias de possíveis meios pelos quais a *Internet* é utilizada por grupos terroristas, entre elas o ‘ataque cibernético’.

Os ataques cibernéticos praticados por grupos terroristas se destinam, preponderantemente, a prejudicar o funcionamento de redes, sistemas, servidores ou ainda, a infraestrutura crítica, por meio do uso de técnicas avançadas de ataques que possibilitem o acesso não autorizado aos sistemas de informação, com o objetivo de incutir pânico à população e ao governo de prosseguir com seus atuais objetivos políticos e sociais (UN, 2012). Esses ataques, quando não direcionados ao governo, podem ser direcionados às grandes corporações ou marcas que representem ou que sejam intrinsecamente ligadas a um determinado país.

Diversos acontecimentos são noticiados como, por exemplo: i) *Hacker* russo invade sistema de uma estação de tratamento de água de *Springfield* (EUA), destruindo remotamente uma bomba de água e prejudicando a distribuição de água da região (TECMUNDO, 2011); ii) Site da NASA é invadido por um suposto grupo

brasileiro (OLHAR DIGITAL, 2013); iii) Sony sofre ataque cibernético antes de exibirem o filme “A entrevista” (G1, 2014) e iv) Mega ataque a provedor afeta sites como *Twitter*, *Spotify* e CNN. O ataque contou com a ajuda de um *botnet*, que “recruta” todo o tipo de dispositivos vulneráveis publicamente acessíveis na internet, resultando em um ataque DDoS (ZAP, 2016). Observa-se que, com a interconectividade das redes, o terrorismo não mais se limita a ações físicas em locais específicos. Conforme Pinheiro (2015), “ainda estamos muito vulneráveis e a maioria dos líderes públicos e empresariais ainda não tratam o tema da Segurança Digital como prioridade de pauta estratégica”.

A insegurança em um mundo interconectado incute a necessidade do desenvolvimento de estratégias que tenham como objetivo a segurança da informação e a proteção da infraestrutura crítica contra ameaças ligadas a ataques cibernéticos, atividades terroristas e/ou espionagem (RIBEIRO, 2011). Ciente desse cenário de insegurança, o governo brasileiro realiza desde 2007, por meio do TCU, um levantamento da situação de governança de TI na Administração Pública Federal.

O principal objetivo desses levantamentos é coletar informações para a elaboração de um mapa com a situação da governança de TI na Administração Pública Federal. “A governança adequada da área de tecnologia da informação na Administração Pública Federal promove a proteção a informações críticas e contribui para que essas organizações atinjam seus objetivos institucionais [...]” (BRASIL, 2008b, p. 2).

Em atendimento ao item 9.4.3 do Acórdão 2.308/2010 do TCU, a Secretaria de Fiscalização de Tecnologia da Informação determinou que processo de trabalho para avaliação da governança de TI na APF ocorreria em ciclos de dois anos.Dessa maneira, o atual levantamento da governança de TI na Administração Pública Federal é do ano de 2014, constante no Acórdão 3.117/2014.

Conforme o Acórdão 3.117/2014 foram selecionadas 373 organizações públicas federais, tendo como critério principal a representatividade no orçamento da União e a autonomia de governança de TI. As organizações selecionadas foram divididas em seis grupos da seguinte maneira:

i) **EXE-Dest**: empresas públicas federais e as sociedades de economia mista;

ii) **EXE-Sisp**: organizações que fazem parte do Sistema de Administração dos Recursos de Informação e Informática (Sisp);

iii) **JUD**: organizações que fazem parte do Poder Judiciário;

iv) **LEG**: organizações que fazem parte do Poder Legislativo;

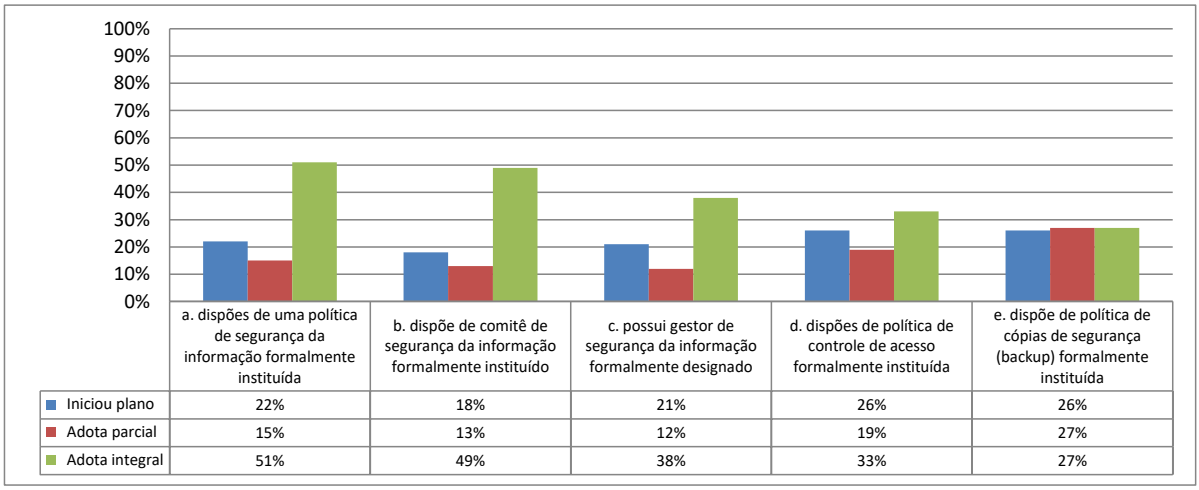
v) **MPU**: organizações que fazem parte do Ministério Público da União (MPU);

vi) **Terceiro Setor**: organizações que não se enquadram em nenhum dos segmentos anteriores.

Essa divisão tem o objetivo de facilitar a análise das informações e permitir à organização comparar seu desempenho em relação ao seu segmento.

Das dimensões avaliadas pelo TCU, uma que destacamos nesse trabalho é a "Gestão Corporativa da Segurança da Informação". Conforme salientado pelo TCU, nos levantamentos anteriores (2008, 2010 e 2012), a segurança da informação já era um ponto de preocupação por causa da "baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis" (BRASIL, 2014, p. 29), O Gráfico 3 apresenta alguns resultados do levantamento:

Gráfico 3 - Práticas relativas às políticas e responsabilidades de segurança da informação



	a. dispões de uma política de segurança da informação formalmente instituída	b. dispõe de comitê de segurança da informação formalmente instituído	c. possui gestor de segurança da informação formalmente designado	d. dispões de política de controle de acesso formalmente instituída	e. dispõe de política de cópias de segurança (backup) formalmente instituída
Iniciou plano	22%	18%	21%	26%	26%
Adota parcial	15%	13%	12%	19%	27%
Adota integral	51%	49%	38%	33%	27%

Fonte: TCU – Acórdão 3.117/2014.

Observa-se que das organizações participantes do estudo, apenas 66% (15% parcialmente e 51% integralmente) declararam possuir de uma política de segurança da informação formalmente instituída. Uma política de segurança da Informação é o principal mecanismo de orientação da gestão da segurança da informação.

Somente 62% das organizações (13% parcialmente e 49% integralmente) declararam possuir um Comitê de Segurança da Informação, ou seja, 38% das organizações participantes não dispõem dessa estrutura, o que possivelmente

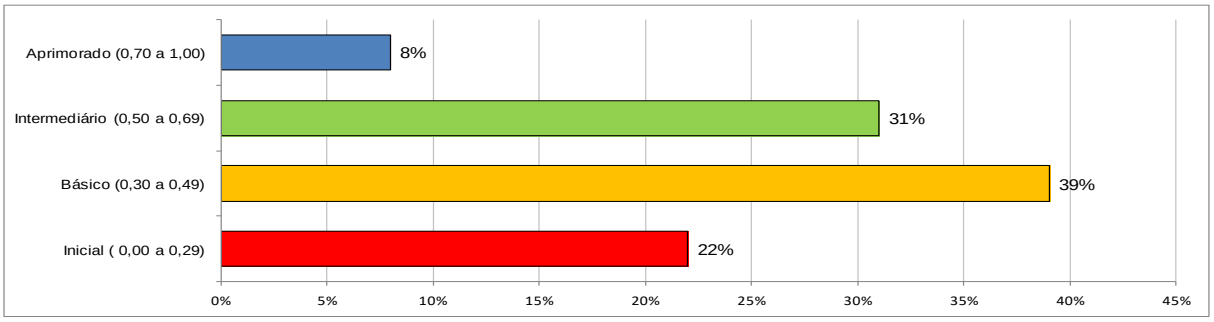
compromete a efetividade das ações de proteção à informação, dado que esse comitê é responsável por “formular e conduzir diretrizes para a segurança da informação corporativa” (BRASIL, 2014).

Em relação à política de controle ao acesso da informação, 48% das organizações não possuem essa política. Conforme a ABNT 27002 (2013), o controle de acesso tem como objetivo limitar o acesso à informação, para que não haja acesso não autorizado a sistemas e serviços. A falta dessa política compromete a segurança da informação, pois usuários não autorizados e/ou ainda mal intencionados serão capazes de acessar, alterar e destruir informações importantes para a continuidade das atividades.

Ainda no levantamento da situação de governança de TI na Administração Pública Federal de 2014 foi mensurado o índice de governança de TI (iGovTI). O iGovTI tem o propósito de orientar as organizações públicas no esforço de melhoria da governança e da gestão de TI. O iGovTI possibilita a verificação do panorama geral da capacidade que as organizações da APF possuem de gerir com eficiência seus ativos de TI, apresentando o estágio de **capacidade de gerenciamento de TI** em que se encontram.

O iGovTI define quatro estágios de capacidade, a saber: i) **Inicial**: iGovTI menor que 0,30; ii) **Básico**: iGovTI maior ou igual a 0,30 e menor que 0,50; iii) **Intermediário**: iGovTI maior ou igual a 0,50 e menor que 0,7; iv) **Aprimorado**: iGovTI maior ou igual a 0,7. O Gráfico 4 apresenta o estágio de desenvolvimento das organizações da APF em governança de TI (iGovTI) de 2014.

Gráfico 4 - iGovTI 2014 – Estágio de Governança de TI



Fonte: TCU – Acórdão 3.117/2014.

Destaca-se do Gráfico 4, que 61% (22% inicial e 39% básico) das organizações da APF não apresentam capacidade adequada de governança e

gestão de TI. Conforme comentado anteriormente, uma governança adequada de TI promove a proteção a informações críticas e contribui para que os objetivos das organizações sejam atingidos. A falta ou baixa capacidade na gestão de TI revela a "existência de lacunas na coordenação e na normatização da gestão corporativa da segurança da informação e que expõe a APF a diversos riscos, como indisponibilidade de serviços e perda de integridade de informações" (BRASIL, 2014, p. 32).

O levantamento do TCU apurou que 87% das organizações, que compuseram o levantamento, disponibilizam algum tipo de serviço por meio da internet, o que indica a importância da gestão da TI na facilitação e melhora da relação entre estado e cidadão. Mas, conforme apresentado no Gráfico 4, há 227 (61%) organizações, entre as 373 que fizeram parte do levantamento, que não possuem adequada governança de TI. Dessa forma, se conjecturarmos que, daquele número, todas disponibilizarem informações e serviços pela rede, então se infere que poderá ocorrer o comprometimento da informação em seus pilares básicos de segurança (disponibilidade, integridade e confidencialidade) na maioria das organizações do estudo, ocasionado pela falta ou inadequação dos mecanismos utilizados para assegurar a informação.

Qualquer organização conectada em uma rede pública ou privada estará sempre sujeita a diversos tipos de ataques eletrônicos. A compreensão da existência de um ambiente virtual inseguro e das possíveis maneiras de ser atacado é necessária para que possam ser aplicadas as devidas proteções e políticas de segurança que impeçam o comprometimento da segurança da informação.

3 METODOLOGIA

O método, segundo Aquino (2013) caracteriza a maneira de como a prática da pesquisa é exercida. Ainda segundo a autora, o fazer ciência consiste em, com rigor, “exercer a prática científica com eficiência e [...] aplicar um método a uma prática” (AQUINO, 2013, p. 28). Dessa maneira, esse capítulo descreve os procedimentos metodológicos adotados para o desenvolvimento da pesquisa. Apresenta, também, sua caracterização, população e amostra e instrumento para a coleta de dados.

3.1 CARACTERIZAÇÃO DA PESQUISA

Quanto aos objetivos, esse estudo se classifica como descritiva, pois descreve, teoricamente, as características do governo eletrônico, suas vantagens e desafios e ainda, expõe os conceitos de segurança da informação e sua importância para a adequada proteção dos sistemas e informações, além de descrever as vulnerabilidades identificadas na coleta de dados e propor soluções. Michel (2015) ressalta que a pesquisa descritiva verifica, descreve e explica problemas, fatos ou fenômenos da vida real, observando e fazendo relações, e ainda faz em geral, levantamentos das características de uma população, um fenômeno ou um fato.

Quanto aos procedimentos, é classificada como documental, pois se utiliza de material ou conteúdo publicado nos portais de governo eletrônico. Os portais de governo eletrônico são considerados documentos, pois conforme Ramos (2009, p. 183), “[...] considera-se documento qualquer informação sob forma de textos, imagens, sons, pintura e outros [...]”.

Quanto à abordagem do problema, caracteriza-se como uma pesquisa quantitativa, pois fará a análise numérica dos dados coletados representando-os por meio de gráficos, tabelas e/ou ilustrações. Para Raupp e Beuren (2004, p. 94), a abordagem quantitativa é “frequentemente utilizada em estudos descritivos, haja vista que se busca classificar a associação entre variáveis e a relação de causalidade entre fenômenos”. Os resultados apurados de vulnerabilidades são analisados e, consequentemente, sugeridas medidas para minimizar os riscos identificados com base na revisão de literatura. Não foi possível implementar uma

análise qualitativa nos resultados devido aos prazos *versus* tamanho da amostra utilizada nesse estudo.

3.2 POPULAÇÃO E AMOSTRA

Inicialmente, considerou-se como população as cinco cidades com maior representatividade no PIB do Estado da Paraíba. De acordo com o Instituto de Desenvolvimento Municipal e Estadual (IDEME, 2016), essas cidades, por ordem de participação no PIB, são: João Pessoa (32,0%), Campina Grande (14,1%), Cabedelo (4,5%), Santa Rita (4,1%) e Patos (2,5%). Juntas, essas cidades representam mais da metade da riqueza produzida no estado da Paraíba.

No entanto, segundo o Instituto Brasileiro de Geografia e Estatística (IBGE, 2016), a Paraíba possui 223 municípios. Dessa maneira, considerar apenas cinco cidades para o estudo seria estatisticamente pouco representativo. Sendo assim, considerou-se, como população da pesquisa, os 50 municípios que representam maior participação para a composição do PIB. Esses 50 municípios representam 83,4% do Produto Interno Bruto do Estado da Paraíba.

A amostra consistiu de todos os municípios que possuem portais de governo eletrônico. O Quadro 5 especifica os municípios que fizeram parte dessa população.

Quadro 5 - Os 50 primeiros municípios que compõe o PIB do Estado da Paraíba

MUNICÍPIO	POSIÇÃO	MUNICÍPIO	POSIÇÃO
João Pessoa	1º	Itaporanga	26º
Campina Grande	2º	Rio Tinto	27º
Cabedelo	3º	Solânea	28º
Santa Rita	4º	Pocinhos	29º
Patos	5º	Mataraca	30º
Bayeux	6º	Areia	31º
Sousa	7º	Bananeiras	32º
Cajazeiras	8º	Princesa Isabel	33º
Guarabira	9º	Cuité	34º
Alhandra	10º	Boqueirão	35º
Conde	11º	São José de Piranhas	36º
Mamanguape	12º	Lucena	37º
Caaporã	13º	Mari	38º
Sapé	14º	Santa Luzia	39º
Pedras de Fogo	15º	Piancó	40º
Queimadas	16º	Pitimbu	41º
Esperança	17º	Soledade	42º
Monteiro	18º	Picuí	43º

Pombal	19º	Remígio	44º
São Bento	20º	São João do Rio do Peixe	45º
Catolé do Rocha	21º	Itapororoca	46º
Alagoa Nova	22º	Belém	47º
Lagoa Seca	23º	Uiraúna	48º
Itabaiana	24º	Sumé	49º
Alagoa Grande	25º	Boa Vista	50º

Fonte: Elaborado pelo autor com base nos dados do IDEME (2016).

Tendo o Quadro 5 como ponto de partida, foram identificados os endereços eletrônicos dos portais de cada município que constituíram a amostra. Os dados foram coletados entre 04 de fevereiro de 2017 e 02 de maio de 2017. Para a coleta dos dados foram utilizados dois computadores do Laboratório de Tecnologia da Informação e o computador pessoal do pesquisador.

Identificou-se que todos os municípios da população, no momento da coleta, possuíam endereço eletrônico com extensão “gov.br”. Apesar disso, somente em 40 municípios foi possível analisar o endereço eletrônico por meio do *software* Netsparker. Dessa maneira, dos 50 endereços de governo eletrônico constantes na população, somente 80% conseguiram ser testados. O Quadro 6 apresenta os municípios que fazem parte da amostra e o respectivo histórico de desenvolvimento do tempo de escaneamento realizada pelo Netsparker.

Quadro 6 - Municípios da amostra e histórico do tempo de escaneamento

MUNICÍPIO	TEMPO DE ESCANEAMENTO	MUNICÍPIO	TEMPO DE ESCANEAMENTO
João Pessoa	38min	Alagoa Grande	1d18h13min
Cabedelo	3h27min	Itaporanga	1h10min
Santa Rita	2d3h49min	Rio Tinto	1d13h43min
Patos	2d4h22min	Solânea	22h07min
Sousa	38min	Pocinhos	52min
Cajazeiras	10h03min	Mataraca	1d20h6min
Guarabira	2h09min	Areia	4d2h12min
Alhandra	10h46min	Bananeiras	4d14h24min
Conde	22h31min	Boqueirão	13h43min
Mamanguape	18h43min	São José de Piranhas	5h16min
Sapé	16min	Lucena	6h26min
Pedras de Fogo	1d14h48min	Mari	2d22min
Queimadas	23h11min	Santa Luzia	13h32min
Esperança	02min	Soledade	4d11h55min
Pombal	14h07min	Picuí	9h05min
São Bento	22h52min	Remígio	02min
Catolé do Rocha	3h12min	São João Rio do Peixe	14h46min
Alagoa Nova	01min	Belém	1d5h56min

Lagoa Seca	02min	Uiraúna	6h24min
Itabaiana	09h20min	Sumé	3h30min

Fonte: Dados da pesquisa (2017).

Os municípios excluídos da população foram: Bayeux, Boa Vista, Caaporã, Campina Grande, Cuité, Itapororoca, Monteiro, Piancó, Pitimbu e Princesa Isabel.

3.3 INSTRUMENTO PARA A COLETA DE DADOS

O instrumento para a coleta de dados, ou seja, a ferramenta utilizada para a verificação da existência de vulnerabilidades nos portais de governo eletrônico, foi o *software* Netsparker.

O Netsparker é um *scanner* de vulnerabilidades. Um *scanner* de vulnerabilidades é um sistema computacional que usa um "[...] método automatizado para identificar vulnerabilidades em elementos e sistemas de rede" em que cada "um dos ativos pertencentes ao escopo da varredura é testado contra uma série de fraquezas conhecidas para a plataforma específica" (UTO, 2013, p. 37). Com base nas informações coletadas é possível associar as possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados (CERT.BR, 2012).

Especificamente, o Netsparker identifica vulnerabilidades e falhas de segurança existentes em aplicações *Web* (*Websites*). Por meio da *Uniform Resource Locator* (URL), que é o endereço de identificação de uma página eletrônica na *Web* como por exemplo <*http://www.joaopessoa.pb.gov.br*>, o Netsparker faz uma varredura no endereço especificado e em todos os links e camadas constantes no referido endereço a procura de vulnerabilidades que possam comprometer a segurança desse sítio na *Internet*.

A ferramenta se utiliza de bancos de dados de vulnerabilidades já conhecidas e executa uma série de verificações ativas para fazer uma melhor estimativa sobre quais vulnerabilidades estão presentes no sistema de um cliente. Conforme Whitman e Mattord (2012), os *scanners* de vulnerabilidade são normalmente usados como parte de um protocolo de ataque para coletar informações que um invasor precisaria para iniciar um ataque bem-sucedido.

As possíveis vulnerabilidades identificadas pelo Netsparker são os dados que compõem essa pesquisa. O *scanner* se utiliza de um banco de dados de vulnerabilidades já conhecidas. Dentre as várias organizações responsáveis por

monitorar e formar essa base de dados de vulnerabilidades cita-se, como exemplo, a organização *Open Web Application Security Project* (OWASP), que faz um levantamento trienal sobre as vulnerabilidades encontradas em aplicações *Web.* No Quadro 7 apresenta-se as 10 vulnerabilidades mais críticas em aplicações *Web* identificadas pela OWASP no relatório trienal de 2013.

Quadro 7 - Top 10 – Vulnerabilidades (OWASP)

POSIÇÃO	VULNERABILIDADE
1	Injection
2	Broken Authentication and Session Management
3	Cross-Site Scripting (XSS)
4	Insecure Direct Object References
5	Security Misconfiguration
6	Sensitive Data Exposure
7	Missing Function Level Access Control
8	Cross-Site Request Forgery (CSRF)
9	Using Known Vulnerable Components
10	Unvalidated Redirects and Forwards

Fonte: Elaborado pelo autor com base nos dados da OWASP (2017).

Tais vulnerabilidades, após a varredura, são classificadas pelo grau de criticidade, ou seja, as vulnerabilidades são agrupadas em categorias de acordo com o risco que representam para o comprometimento da segurança dos portais governamentais analisados. Os graus de criticidade são divididos em cinco níveis, sendo eles: 1) Crítica, 2) Alta Criticidade, 3) Média Criticidade, 4) Baixa Criticidade e 5) Alertas e Informações, sendo a Crítica a de maior risco. Quanto mais alto o nível de classificação de criticidade da vulnerabilidade detectada maior é a facilidade de acesso indevido aos portais de governo eletrônico.

4 ANÁLISE E DESCRIÇÃO DOS RESULTADOS

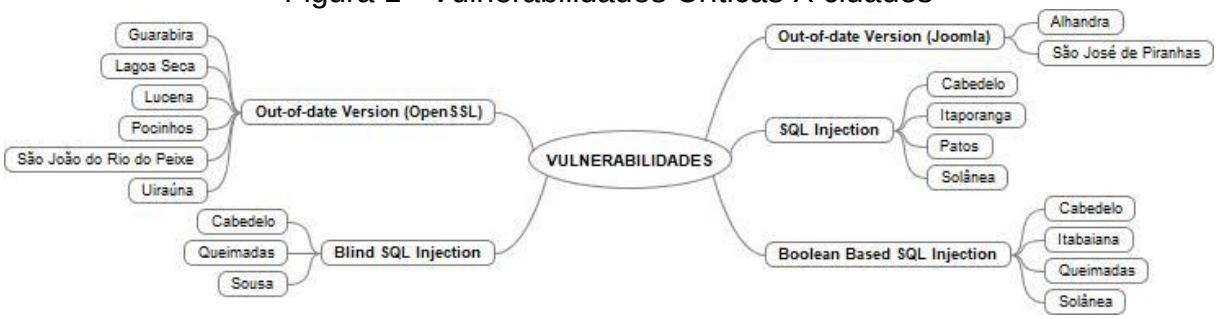
Esta seção apresenta os resultados obtidos da varredura feita pelo *software* Netsparker que identificou as vulnerabilidades existentes. Nos portais de governo eletrônico as vulnerabilidades descritas a partir desse ponto, não necessariamente apresentaram apenas uma ocorrência, podendo ter havido várias ocorrências da mesma vulnerabilidade em único endereço eletrônico (*site*) analisado.

Apresentam-se os resultados por nível de criticidade, a saber: 1) Crítica, 2) Alta Criticidade e 3) Média Criticidade, por apresentarem maior urgência em suas correções. Os níveis de: 4) Baixa Criticidade e 5) Alertas e Informações estão dispostos nos apêndices (A e B), pois sua correção muitas vezes depende de uma análise do custo e benefício por não apresentarem ameaças que comprometam a continuidade do serviço.

4.1 VULNERABILIDADES CRÍTICAS

As vulnerabilidades Críticas são vulnerabilidades cuja exploração pode levar ao comprometimento em larga escala da infraestrutura de TI. “São brechas facilmente exploradas, pois o hacker não precisa de nenhuma credencial especial e nem precisa persuadir um usuário. Esse tipo de falha precisa ser remediado o mais rápido possível.” (IBLISS, 2016, p. 4). Abaixo, a Figura 1 resume as vulnerabilidades Críticas encontradas e aos respectivos portais das cidades associadas a cada vulnerabilidade.

Figura 1 - Vulnerabilidades Críticas X cidades



Fonte: Dados da pesquisa (2017).

4.1.1 Vulnerabilidade Out-of-date Version (Joomla)

O *Joomla* é um sistema de gerenciamento de conteúdo de código aberto para a publicação de conteúdo da *Web*. O Netsparker identificou que alguns sites pesquisados estão usando o código *Joomla* e detectou que o mesmo encontra-se desatualizado.

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre as vulnerabilidades encontradas da desatualização do *Joomla*, destacam-se:

a. ***Joomla CSRF Vulnerability***: permite que atacantes remotos sequestrem a autenticação de vítimas não especificadas para pedidos que carregam o código via vetores desconhecidos. CSRF é um ataque que engana a vítima para enviar uma solicitação maliciosa. Ele herda a identidade e privilégios da vítima para desempenhar uma função indesejada em nome da vítima.
b. ***Joomla SQL Injection Vulnerability:*** permite que um usuário remoto não autorizado obtenha privilégios de administrador sequestrando a sessão de administrador. Após a exploração da vulnerabilidade, o invasor pode obter o controle total do site e executar ataques adicionais.
c. ***Joomla Sensitive Information Disclosure:*** um invasor pode obter informações confidenciais ou ignorar certas restrições de segurança e executar ações não autorizadas.
d. ***Joomla! Multiple XSS Vulnerabilities:*** essa vulnerabilidade refere-se ao ataque de injeção de código do lado do cliente, em que um invasor pode executar *scripts* maliciosos. O invasor explora uma vulnerabilidade dentro de um site ou aplicativo da *Web* que a vítima visita, usando essencialmente o site vulnerável como veículo para entregar um *script* malicioso ao navegador da vítima.

A solução para a correção dessa vulnerabilidade consiste na atualização da plataforma de gerenciamento de conteúdo *Joomla* para a sua versão mais recente.

As cidades que apresentaram essa vulnerabilidade foram: Alhandra e São José de Piranhas. Essa vulnerabilidade está classificada como Crítica em conformidade com as organizações OWASP (2013), PCI (2016) e CAPEC (2017).

4.1.2 Out-of-date Version (OpenSSL)

O *OpenSSL* é um código aberto do padrão *Secure Socket Layer* (SSL) usado em inúmeros servidores *web*. O SSL é um protocolo que ao invés de transmitir os pacotes em texto simples, legível por humanos, permite que as informações sejam criptografadas utilizando algoritmos, ou seja, as informações só deverão ser lidas apenas pelo usuário a quem se destina a mensagem, não sendo possível que durante o tráfego da informação, usuários não autorizados tenham acesso aos dados. O Netsparker identificou que alguns sites pesquisados estão usando o *OpenSSL* e detectou que o mesmo encontra-se desatualizado.

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***OpenSSL Denial of Service Vulnerability:*** esse tipo de ataque tem como objetivo a negação de serviço (DoS), ou seja, um invasor tenta impedir que usuários legítimos acessem informações ou serviços. Quando você digita um URL para um determinado site no seu navegador, você está enviando uma solicitação para o servidor do computador desse site para exibir a página. O servidor só pode processar um certo número de requisições ao mesmo tempo, portanto, se um invasor sobrecarregar o servidor com solicitações, ele não poderá processar sua solicitação. Esta é uma "negação de serviço" porque você não pode acessar esse site.

b. ***OpenSSL TLS Heartbeart Read Overrun Vulnerability:*** essa vulnerabilidade permite que informações protegidas sejam roubadas da comunicação criptografada SSL / TLS, ou seja, um invasor é capaz de acessar dados previamente alocados na memória e que pode incluir desde *cookies* de sessão à chaves privadas (que são usadas para a segurança da comunicação entre dois computadores).

c. ***OpenSSL Information Disclosure Vulnerability:*** ao atacar um servidor que usa uma versão vulnerável do *OpenSSL*, um invasor remoto não autenticado pode recuperar informações confidenciais, como senhas secretas. Ao alavancar essas informações, um invasor pode ser capaz de descriptografar, falsificar ou executar ataques *man-in-the-middle* no tráfego de rede que de outra forma seriam protegidos pelo *OpenSSL*.

A solução para a correção dessa vulnerabilidade consiste na atualização do código *OpenSSL* para a sua versão mais recente.

As cidades que apresentaram essa vulnerabilidade foram: Guarabira, Lagoa Seca, Lucena, Pocinhos, São José do Rio do Peixe e Uiraúna. Essa vulnerabilidade está classificada como Crítica em conformidade com as organizações OWASP (2013), PCI (2016) e CAPEC (2017).

4.1.3 SQL Injection / Blind SQL Injection / Boolean Based SQL Injection

Nesse tópico apresentam-se três vulnerabilidades Críticas baseadas na linguagem de programação SQL, cuja diferença entre cada uma das vulnerabilidades é a técnica utilizada para a sua exploração. Nesse caso específico, a correção da vulnerabilidade é a mesma para as três vulnerabilidades Críticas encontradas.

4.1.3.1 SQL Injection

A SQL é uma linguagem de programação projetada para gerenciar dados armazenados em um Sistema de Gerenciamento de Banco de Dados Relacional (RDBMS), portanto SQL pode ser usado para acessar, modificar e excluir dados.

A *SQL Injection* é uma técnica de ataque baseada na manipulação do código SQL que visa comprometer a segurança da base de dados por meio de comandos inseridos nos campos de formulários ou URL. Um ataque bem sucedido permite o acesso aos dados confidenciais dos usuários presentes no banco de dados do sistema/aplicação, ou seja, através de uma manipulação forçada do código SQL é possível que um atacante consiga acesso ao sistema se fazendo passar por um usuário real. É possível também que o atacante manipule ou até destrua os dados presentes no banco de dados, impossibilitando que usuários antes cadastrados, não tenham mais o devido acesso.

O OWASP (2013) alerta que *SQL Injections* podem resultar em perda ou corrupção de dados, falta de responsabilização, ou negação de acesso. Algumas vezes, a injeção pode levar ao comprometimento completo do servidor.

As cidades que apresentaram essa vulnerabilidade foram: Cabedelo, Itaporanga, Patos e Solânea. Essa vulnerabilidade está classificada como Crítica em

conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.1.3.2 Blind SQL Injection

A *Blind SQL Injection* se assemelha à *SQL Injection*, a única diferença é a forma como os dados são recuperados do banco de dados. Quando o site é configurado para mostrar mensagens de erro genéricas (erro padrão HTTP 500 ou 404) e o banco de dados não fornece dados para a página da *Web*, um invasor é forçado a roubar dados, perguntando ao banco de dados uma série de perguntas verdadeiras ou falsas. É possível também que o atacante manipule ou até destrua os dados presentes no banco de dados, impossibilitando que usuários antes cadastrados, não tenham mais o devido acesso.

O OWASP (2013) alerta que *SQL Injections* podem resultar em perda ou corrupção de dados, falta de responsabilização, ou negação de acesso. Algumas vezes, a injeção pode levar ao comprometimento completo do servidor.

As cidades que apresentaram essa vulnerabilidade foram: Cabedelo, Queimadas e Sousa. Essa vulnerabilidade está classificada como Crítica em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.1.3.3 Boolean Based SQL Injection

A técnica de exploração booleana é muito útil quando o testador encontra uma situação de *Blind SQL Injection*, na qual nada é conhecido sobre o resultado de uma operação. Por exemplo, esse comportamento ocorre nos casos em que o programador criou uma página de erro personalizada que não revela nada na estrutura da consulta ou no banco de dados. (a página não retorna um erro SQL, ela retorna um erro padrão HTTP 500 ou 404, ou ainda realiza o redirecionamento). Usando métodos de inferência, é possível evitar este obstáculo e assim obter êxito na recuperação dos valores de alguns campos desejados. Este método consiste em realizar uma série de consultas booleanas contra o servidor, observando as respostas e, finalmente, deduzindo o significado de tais respostas.

Aqui também a manipulação dos códigos SQL em um possível ataque, caso bem sucedido, permite ao atacante o acesso ao banco de dados do site onde, dessa maneira, terá acesso aos dados confidenciais do usuário, podendo alterá-los ou excluí-los. O OWASP (2013) alerta que Injeção pode resultar em perda ou corrupção de dados, falta de responsabilização, ou negação de acesso. Algumas vezes, a injeção pode levar ao comprometimento completo do servidor.

As cidades que apresentaram essa vulnerabilidade foram: Cabedelo, Itabaiana, Queimadas e Solânea. Essa vulnerabilidade está classificada como Crítica em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

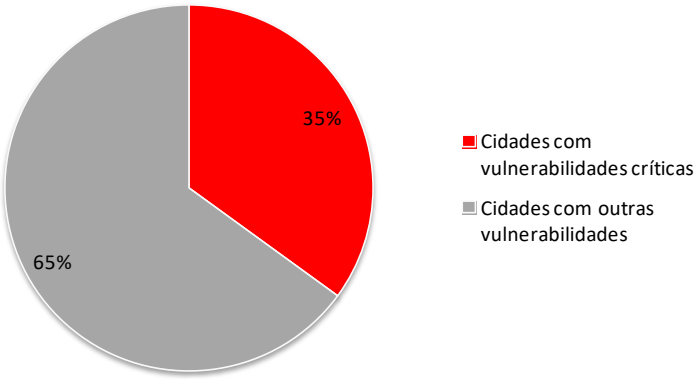
Conforme o OWASP (2013), a solução para a correção das três vulnerabilidades baseadas no código SQL consiste em:

- Utilizar uma Interface (API) segura que evite o uso do interpretador inteiramente ou forneça uma interface parametrizada.
- caso uma API parametrizada não esteja disponível, deve-se filtrar cuidadosamente os caracteres especiais utilizando a sintaxe para esse interpretador.
- “lista branca" ou validação de entrada positiva também é recomendada, mas não é uma defesa completa já que muitas aplicações requerem caracteres especiais em suas entradas.

4.2 CONCLUSÃO DO TÓPICO (vulnerabilidades Críticas)

Na varredura, foram encontradas cinco vulnerabilidades Críticas nos portais das cidades analisadas. Ressalta-se que, das 40 cidades participantes da amostra, 14 cidades apresentaram pelo menos uma vulnerabilidade Crítica (Gráfico 5).

Gráfico 5 - Vulnerabilidades Críticas



Fonte: Dados da pesquisa (2017).

As cidades que apresentaram pelo menos uma vulnerabilidade Crítica representam 35% da amostra. Dentre as cinco vulnerabilidades Críticas encontradas pelo software Netsparker, o município de Cabedelo apresentou o maior número de ocorrências (três vulnerabilidades Críticas encontradas).

Um ponto importante a ressaltar é que três vulnerabilidades Críticas encontradas na varredura, o *SQL Injection*, o *XSS* (*cross-site scripting*) e o *CSRF* (*cross-site request forgery*), estão incluídas, segundo o relatório da OWASP (2013), entre os dez riscos de segurança mais severos em aplicações *Web*.

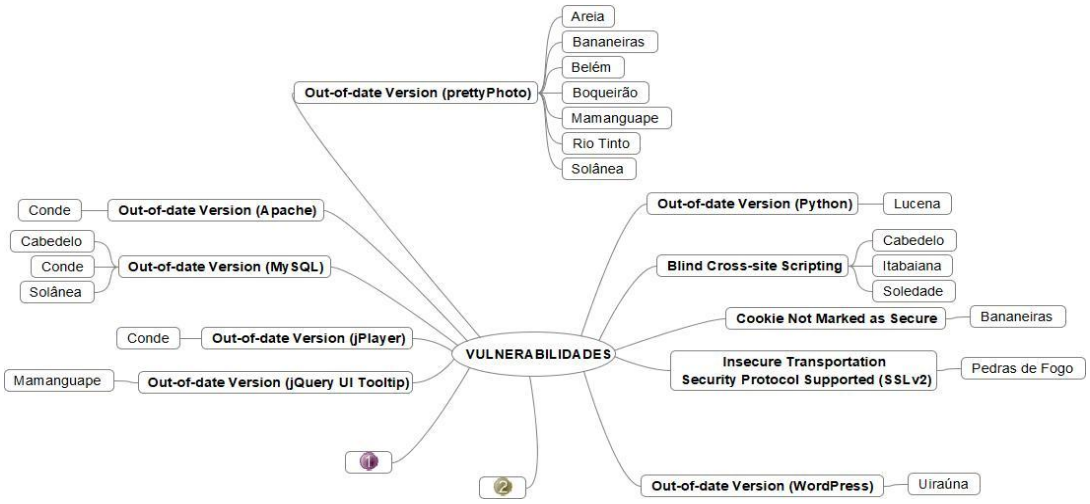
Tais vulnerabilidades permitem invasão aos sites dos municípios. Essa invasão pode comprometer gravemente a continuidade do serviço bem como permitir a exposição e uso não autorizado de dados privados dos diversos usuários. Vulnerabilidades consideradas de nível crítico devem ser corrigidas imediatamente a fim de diminuir as possibilidades de comprometimento da segurança da informação.

4.3 VULNERABILIDADES DE ALTA CRITICIDADE

As vulnerabilidades de Alta Criticidade são geralmente de “mais difícil exploração, mas podem levar a problemas como elevação de privilégios, perda de dados” e que permitem o “acesso remoto à rede, erro que pode levar ao roubo de dados e à paralisação de processos fundamentais” (IBLISS, 2016, p. 4). A Figura 2 resume as vulnerabilidades de Alta Criticidade encontradas e as respectivas cidades associadas a cada vulnerabilidade. Por ocorrerem em muitas cidades, as

vulnerabilidades ligadas aos números 1 e 2, inseridos na Figura 2, serão listadas no Quadro 8.

Figura 2 - Vulnerabilidades de Alta Criticidade X cidades



Fonte: Dados da pesquisa (2017).

Quadro 8 - Vulnerabilidades de Alta Criticidade

VULNERABILIDADE 1	VULNERABILIDADE 2
Password Transmitted over HTTP	**Cross-site Scripting**
Alagoa Grande	Alhandra
Alhandra	Bananeiras
Areia	Itabaiana
Bananeiras	Itaporanga
Belém	Lucena
Boqueirão	Patos
Cabedelo	Pombal
Cajazeiras	Queimadas
Catolé	Sapé
Conde	Solânea
Itaporanga	Uiraúna
Mamanguape	
Mari	
Mataraca	
Patos	
Pedras de Fogo	
Pombal	
Rio Tinto	
Santa Luzia	
Santa Rita	
São Bento	
São João do Rio do Peixe	
São José de Piranhas	
Sapé	
Soledade	
Uiraúna	

Fonte: Dados da pesquisa (2017).

4.3.1 Cross-site Scripting (XSS)

Conforme a OWASP (2016) o *Cross-site Scripting* (XSS) refere-se ao ataque de injeção de código do lado do cliente, em que um invasor pode executar *scripts* maliciosos em um site ou aplicativo *web*. Ao executar o XSS, um atacante não tem como alvo uma vítima diretamente. Em vez disso, um invasor explora uma vulnerabilidade dentro de um *site* ou aplicativo da *Web* que a vítima visita, usando essencialmente o site vulnerável como veículo para entregar um *script* malicioso ao navegador da vítima.

O navegador do usuário final entende que o *script* veio de uma fonte confiável, o que permite que esse *script* mal-intencionado possa acessar todos os *cookies*, *tokens* de sessão ou outras informações confidenciais retidos pelo navegador (OWASP, 2016).

Conforme o OWASP (2013, p. 10), a solução para a correção dessa vulnerabilidade consiste em:

> a. Filtrar adequadamente todos os dados não-confiáveis com base no contexto HTML (corpo, atributo, *JavaScript*, CSS ou URL) no qual os dados serão colocados.
> b. “Lista branca" ou validação de entrada positiva também é recomendada, pois ajuda a proteger contra XSS, mas não é uma defesa completa, já que muitas aplicações requerem caracteres especiais em sua entrada.
> c. Considerar bibliotecas de auto-sanitização como OWASP's AntiSamy ou o Java HTML Sanitizer Project.
> d. Considerar a *Content Security Policy* (CSP) para se defender contra XSS em todo o site.

As cidades que apresentaram essa vulnerabilidade foram: Alhandra, Bananeiras, Itabaiana, Itaporanga, Lucena, Patos, Pombal, Queimadas, Sapé, Solânea e Uiraúna. Essa vulnerabilidade está classificada como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.3.2 Password Transmitted over HTTP

O Netsparker detectou que os dados relativos as senhas estão sendo transmitidos pela conexão HTTP. Isso significa que quando você digita uma senha em um *site*, essa não é enviada por meio de uma conexão criptografada, o que permite sua captura.

O atacante que capturar a senha terá todos os privilégios relativos ao usuário que teve a senha capturada, podendo excluir dados, modificar cadastro e ter acesso a todos os dados cadastrados pelo usuário no respectivo *site*.

A solução para a correção dessa vulnerabilidade, conforme o OWASP (2013) consiste em:

a. Criptografar todos os dados sensíveis em repouso e em trânsito.
b. Não armazenar dados sensíveis desnecessariamente.
c. Certificar-se que o nível utilizado nos algoritmos e chaves são fortes, e que o gerenciamento de chaves está aplicado adequadamente.
d. Desabilitar o autocompletar em formulários de coleta de dados sensíveis e desabilitar o *cache* em páginas que contenham dados sensíveis.

As cidades que apresentaram essa vulnerabilidade foram: Alagoa Grande, Alhandra, Areia, Bananeiras, Belém, Boqueirão, Cabedelo, Cajazeiras, Catolé, Conde, Itaporanga, Mamanguape, Mari, Mataraca, Patos, Pedras de Fogo, Pombal, Rio Tinto, Santa Luzia, Santa Rita, São Bento, São João do Rio do Peixe, São José de Piranhas, Sapé, Soledade e Uiraúna. Essa vulnerabilidade está classificada como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.3.3 Versões desatualizadas

Esse tópico apresenta as vulnerabilidades de Alta Criticidade, relativas às desatualizações, identificadas pelo Netsparker, de versões de linguagens de programação e/ou *scripts*.

4.3.3.1 Out-of-date Version (PHP)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes, entre as quais, destacam-se:

a. ***PHP Denial of Service Vulnerability****:* permite que atacantes remotos causem uma negação de serviço ou possivelmente ter outro impacto não especificado através de vetores desconhecidos.
b. ***PHP Code Execution Vulnerability****:* permite que atacantes remotos obtenham informações confidenciais da memória.

4.3.3.2 Out-of-date Version (prettyPhoto)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destaca-se:

a. ***Cross-site Scripting (XSS):*** permite que os invasores remotos injetem *scripts* via *web.*

4.3.3.3 Out-of-date Version (MySQL)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***Oracle MySQL Server CVE-2012-3158 Remote Security Vulnerability***: permite que atacantes remotos afetem a confidencialidade, integridade e disponibilidade através de vetores desconhecidos relacionados ao Protocolo.
b. ***Oracle January 2014 Critical Patch Update Multiple Vulnerabilities***: permite que usuários remotos autenticados afetem a disponibilidade via vetores desconhecidos relacionados a uma lista de produtos de software da empresa Oracle, que vão desde sistemas gerenciadores de banco de dados até linguagens de programação.

4.3.3.4 Out-of-date Version (Apache)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***Apache mod_cache and mod_dav Request Handling Denial of Service Vulnerability***: permite que atacantes remotos causem uma negação de serviço através de um pedido que não tem um caminho.
b. ***Apache HTTP Server Scoreboard Local Security Bypass Vulnerability*:** permite que usuários locais causem uma negação de serviço ou possivelmente outro impacto não especificado, ao modificar um determinado campo dentro de um segmento de memória compartilhada.

4.3.3.5 Out-of-date Version (jPlayer)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destaca-se:

a. ***Cross-site Scripting (XSS) Vulnerability***: permite que atacantes remotos injetem *scripts,* via *web,* possivelmente relacionados a listas negras incompletas.

4.3.3.6 Out-of-date Version (Python)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***Python Multiple Denial of Service Vulnerabilities***: permite que atacantes remotos causem uma negação de serviço fechando imediatamente uma conexão TCP.
b. ***Python 'audioop' Module Integer Overflow Vulnerability***: permite que os invasores causem uma negação de serviço (falha do aplicativo).

4.3.3.7 Out-of-date Version (jQuery UI Tooltip)

A desatualização desse código apresenta múltiplas vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destaca-se:

a. ***Autocomplete Cross-site Scripting (XSS) Vulnerability***: permite que invasores remotos injetem *scripts* ou HTML via *Web*, relacionados ao *upload* de arquivos, significando que o módulo de preenchimento automático torna o site vulnerável.

4.3.3.8 Out-of-date Version (WordPress)

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***Wordpress Improper Authentication Vulnerability***: não determina corretamente a validade dos *cookies* de autenticação, o que torna mais fácil para atacantes remotos obterem acesso através de *cookies* falsos.
b. ***Wordpress Denial of Service Vulnerability***: permite que atacantes remotos causem uma negação de serviço.
c. ***Wordpress Information Disclosure Vulnerability***: permite que atacantes remotos obtenham informações confidenciais por meio de uma solicitação de *upload* inválida.

A solução para a correção de todas as vulnerabilidades, decorrentes de desatualizações de códigos e *scripts*, consiste na atualização para as suas versões mais recentes.

As cidades que apresentaram essas vulnerabilidades foram: Alagoa Grande, Areia, Bananeiras, Belém, Boqueirão, Cabedelo, Catolé, Conde, Guarabira, Itabaiana, Itaporanga, João Pessoa, Lucena, Mamanguape, Mari, Mataraca, Patos, Picuí, Rio Tinto, São Bento, Sapé, Solânea, Soledade, Sousa, Sumé e Uiraúna. Essas vulnerabilidades estão classificadas como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016) e CAPEC (2017).

4.3.4 Blind Cross-site Scripting (XSS)

Essa vulnerabilidade permite diferentes tipos de ataque, principalmente o sequestro da sessão atual do usuário ou alterar a aparência da página, alterando o HTML para roubar as credenciais do usuário. Possibilita que invasores sequestrem sessões de outros usuários, inclusive sendo possível o ataque ao administrador para obter controle total sobre o aplicativo.

Esses ataques podem ser executados através do uso de scripts entre sites, permitindo: i) sequestro sessão ativa do usuário, ii) montagem de ataques de *phishing* e iii) interceptação de dados e realização ataques do tipo *man-in-the-middle*.

Os ataques *Cross-site Scripting* mais graves envolvem a divulgação do *cookie* de sessão do usuário, permitindo que um invasor segure a sessão do usuário e tome conta da conta. Outros ataques prejudiciais incluem a divulgação de arquivos de usuários finais, a instalação de programas de cavalos de Tróia, o redirecionamento do usuário para outra página ou site ou a apresentação de conteúdo (OWASP, 2016).

Conforme o OWASP (2013, p. 10), a solução para a correção dessa vulnerabilidade consiste em:

> e. Filtrar adequadamente todos os dados não-confiáveis com base no contexto HTML (corpo, atributo, *JavaScript*, CSS ou URL) no qual os dados serão colocados.
> f. “Lista branca" ou validação de entrada positiva também é recomendada, pois ajuda a proteger contra XSS, mas não é uma defesa completa, já que muitas aplicações requerem caracteres especiais em sua entrada.
> g. Considerar bibliotecas de auto-sanitização como OWASP's *AntiSamy* ou o Java HTML *Sanitizer Project*.
> h. Considerar a *Content Security Policy* (CSP) para se defender contra XSS em todo o site.

As cidades que apresentaram essas vulnerabilidades foram: Cabedelo, Itabaiana e Soledade. Essa vulnerabilidade está classificada como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.3.5 Cookie Not Marked as Secure

Essa vulnerabilidade significa que um *cookie* pode ser potencialmente roubado por um invasor que pode interceptar e descriptografar o tráfego. Este *cookie* será transmitido através de uma conexão HTTP, portanto, se esse *cookie* for importante (como um *cookie* de sessão), um invasor pode interceptá-lo e sequestrar a sessão de uma vítima. O atacante pode realizar um ataque *man-in-the-middle*, podendo forçar a vítima a fazer uma solicitação HTTP para roubar o *cookie*.

Conforme o site *teamtreehouse.com (2017)*, referência externa citada pelo próprio Netsparker, a solução para a correção dessa vulnerabilidade consiste em:

a. Limitar a quantidade de informações confidenciais armazenadas no *cookie*.
b. Limitar os subdomínios e caminhos para impedir a interceptação por outro aplicativo.

c. Implementar a conexão SSL para que o *cookie* não seja enviado em texto não criptografado.

A cidade que apresentou essa vulnerabilidade foi Bananeiras. Essa vulnerabilidade está classificada como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.3.6 Insecure Transportation Security Protocol Supported (SSLv2)

O Netsparker detectou que o protocolo de segurança de transporte inseguro (SSLv2) é suportado pelo servidor *web* do site analisado. Atacantes podem realizar ataques do tipo *man-in-the-middle* e observar o tráfego de criptografia entre o site do município e seus visitantes.

Fornecer proteção de camada de transporte adequada pode afetar o design do site. É mais fácil exigir SSL para todo o site. Por motivos de desempenho, alguns sites usam SSL somente em páginas particulares. Outros usam SSL somente em páginas críticas, mas isso pode expor IDs de sessão e outros dados confidenciais (OWASP, 2010).

Conforme o OWASP (2010), a solução para a correção dessa vulnerabilidade consiste em:

a. Exigir SSL para todas as páginas sensíveis. As solicitações não SSL para essas páginas devem ser redirecionadas para a página SSL.
b. Definir o sinalizador 'seguro' em todos os *cookies* sensíveis.
c. Configurar o provedor de SSL apenas para suportar algoritmos fortes.
d. Certificar-se de que o certificado é válido, não expirado, não revogado e corresponde a todos os domínios usados pelo site.

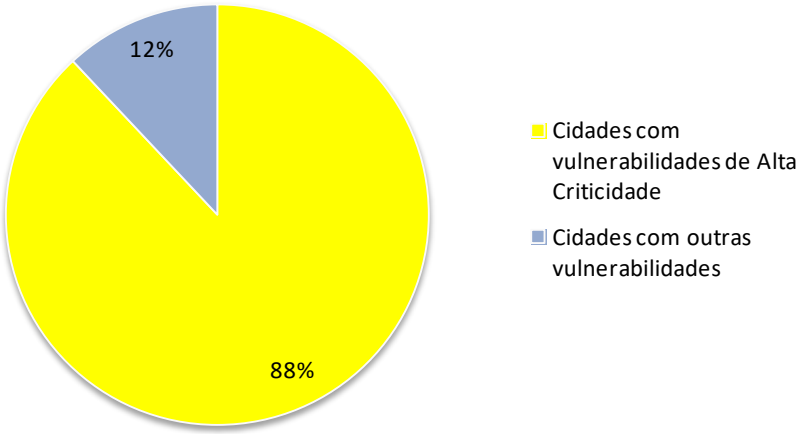
A cidade que apresentou essa vulnerabilidade foi Pedras de Fogo. Essa vulnerabilidade está classificada como de Alta Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017) e CAPEC (2017).

4.4 CONCLUSÃO DO TÓPICO (vulnerabilidades de Alta Criticidade)

Na varredura do software Netsparker, foram encontradas 13 diferentes vulnerabilidades de Alta Criticidade dentre as cidades analisadas. Ressalta-se que,

das 40 cidades participantes da amostra, 35 cidades apresentaram pelo menos uma vulnerabilidade de Alta Criticidade (Gráfico 6).

Gráfico 6 - Vulnerabilidades de Alta Criticidade



Fonte: Dados da pesquisa (2017).

As cidades que apresentaram pelo menos uma vulnerabilidade Alta Criticidade representam 88% da amostra. Dentre as 13 vulnerabilidades de Alta Criticidade encontradas pelo software Netsparker, ressaltam-se as vulnerabilidades *Cross-site Scripting, Password Transmitted over HTTP e Out-of-date Version (PHP)* que estiveram presentes em 11, 26 e 21 cidades respectivamente.

Pode-se comparar a taxa de 88% com o relatório de ameaças do iBLISS (2016), que, ao pesquisar vulnerabilidades no setor privado encontrou que o setor privado de Internet apresenta uma taxa de 66% de vulnerabilidades de Alta Criticidade.

A taxa de 88% do setor público ao ser comparada com a taxa de 66% do setor privado, está em consonância com o *SecurityScorecard R&D Department* (SSD, 2016), o qual foi destacado em seu relatório de cibersegurança, que, quando comparado com o desempenho em cibersegurança de outros segmentos organizacionais (indústrias, prestadores de serviço, financeiras, etc.), as organizações governamentais são as que apresentam o mais alto índice de vulnerabilidades em sua infraestrutura de sistema em nível federal, estadual e municipal.

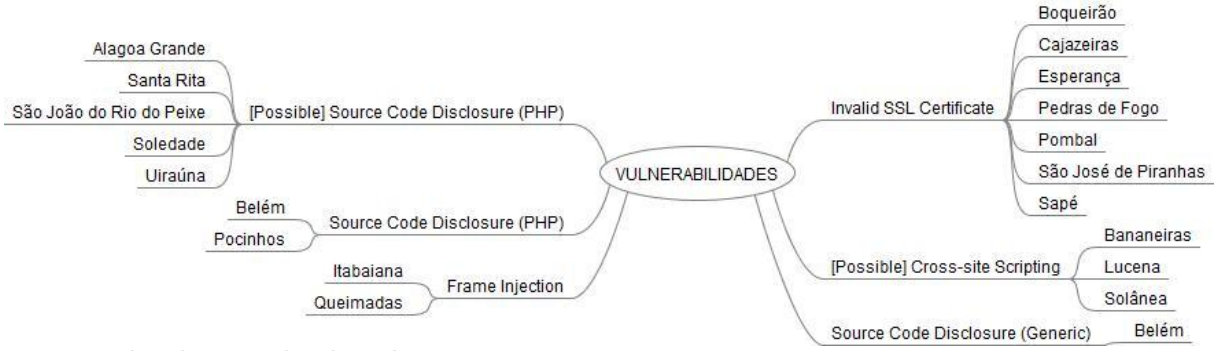
Ressalta-se que três destas vulnerabilidades encontradas na varredura, o C*ross-site Scripting*, o *Blind Cross-site Scripting* e o *Insecure Transportation Security Protocol Supported (SSLv2)* estão incluídas, segundo o relatório da OWASP (2013), entre os dez riscos de segurança mais críticos em aplicações *Web*.

Vulnerabilidades de Alta Criticidade apesar de terem maior dificuldade de exploração, quando comparadas às vulnerabilidades Críticas, ainda podem comprometer a continuidade do serviço, pois permitem que invasores tenham acesso ao controle do site e acessem informações de usuários e administradores. Essas vulnerabilidades possibilitam que atacantes tenham acesso às informações do usuário que são enviadas pela internet ou por meio de conexões *Wi-Fi.* Vulnerabilidades de Alta Criticidade devem ser corrigidas imediatamente a fim de diminuir as possibilidades de comprometimento da segurança da informação.

4.5 VULNERABILIDADES DE MÉDIA CRITICIDADE

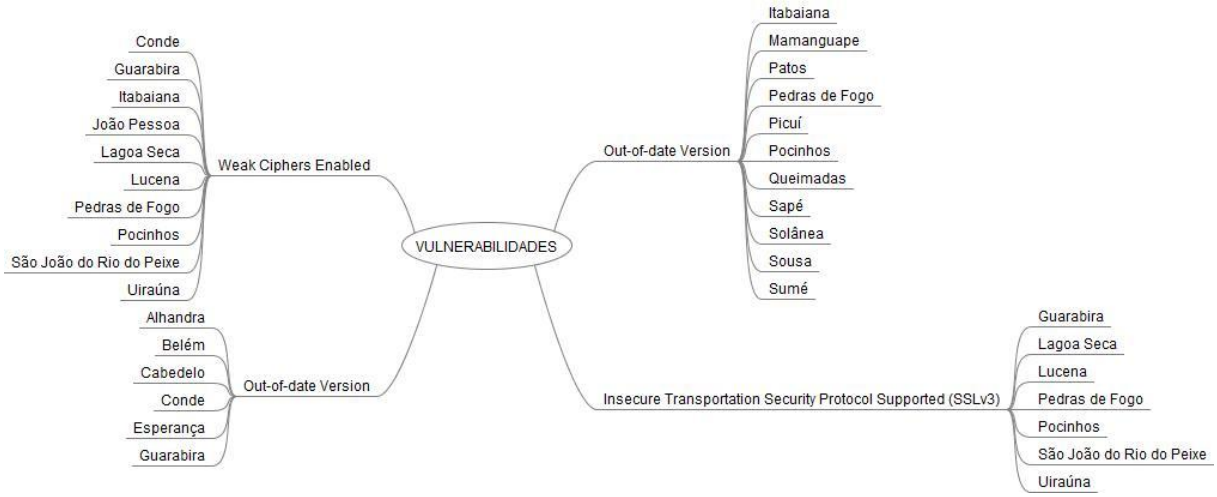
As vulnerabilidades de Média Criticidade conforme o iBLIS (2016, p. 4) “são vulnerabilidades que requerem que o criminoso manipule as vítimas, portanto são mais trabalhosas para o hacker”. Essas falhas geralmente exigem que o cibercriminoso tenha privilégios de usuário. As Figuras 3 e 4 resumem as vulnerabilidades de Média Criticidade encontradas e as respectivas cidades associadas a cada vulnerabilidade.

Figura 3 - Vulnerabilidades de Média Criticidade X cidades



Fonte: Dados da Pesquisa (2017).

Figura 4 - Vulnerabilidades de Média Criticidade X cidades



Fonte: Dados da Pesquisa (2017).

4.5.1 Out-of-date Version (jQuery / jQuery Migrate / WordPress / jQuery UI Dialog)

Por se tratar de vulnerabilidades referentes à desatualização de códigos/programas, esse tópico irá apenas apresentar as vulnerabilidades de Média Criticidade encontradas relativas às versões desatualizadas, sem adentrar em seus aspectos intrínsecos, por já terem sido abordadas em tópicos anteriores e para que não fique repetitivo.

Dessa maneira, as vulnerabilidades de Média Criticidade encontradas decorrentes de desatualizações de códigos/programas foram:

a. ***Out-of-date Version (jQuery)***
b. ***Out-of-date Version (jQuery Migrate)***
c. ***Out-of-date Version (WordPress)***
d. ***Out-of-date Version (jQuery UI Dialog)***
e. ***Out-of-date Version (PHP)***

A solução para a correção de todas as vulnerabilidades, decorrentes de desatualizações de códigos/programas, consiste na atualização para as suas versões mais recentes.

As cidades que apresentaram essas vulnerabilidades foram: Alhandra, Belém, Cabedelo, Conde, Esperança, Guarabira, Itabaiana, Mamanguape, Patos, Pedras de Fogo, Picuí, Pocinhos, Queimadas, Sapé, Solânea, Sousa e Sumé. Essas

vulnerabilidades estão classificadas como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016) e CAPEC (2017).

4.5.2 Invalid SSL Certificate

Um certificado SSL é um padrão global de segurança que tem a finalidade de permitir que os dados transmitidos entre o servidor e o navegador sejam criptografados a fim de garantir a proteção e sigilo dos mesmos.

Um certificado SSL pode ser criado e assinado por qualquer pessoa. O município deve possuir um certificado SSL válido para fazer com que seus visitantes tenham confiança de que há uma comunicação segura entre o site e o navegador. Se o certificado é inválido, os visitantes terão dificuldade em distinguir entre o certificado do site do município e os de possíveis invasores. Um certificado inválido permite que atacantes possam realizar ataques do tipo *man-in-the-middle* e observar o tráfego de criptografia entre o site do município e seus visitantes.

Todos os certificados tem data de vencimento, ou seja, expiram sua validade. A solução para a correção dessa vulnerabilidade consiste na renovação da validade do certificado junto às autoridades certificadoras.

As cidades que apresentaram essas vulnerabilidades foram: Boqueirão, Cajazeiras, Esperança, Pedras de Fogo, Pombal, São José de Piranhas e Sapé. Essas vulnerabilidades estão classificadas como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017) e CAPEC (2017).

4.5.3 Source Code Disclosure (PHP / Generic)

O Netsparker identificou uma possível revelação do código-fonte PHP. Um invasor pode obter o código fonte do servidor do aplicativo da Web, que pode conter dados confidenciais - como sequências de conexão de banco de dados, nomes de usuários e senhas. Conforme a Acunetix (2016), o “código fonte geralmente contém alguma forma de informações confidenciais - sejam informações relacionadas à configuração [...] ou simplesmente informações sobre como funciona a aplicação *Web*”.

Segundo o OWASP (2013), dependendo do código-fonte, a sequência de conexão do banco de dados, o nome de usuário e senhas, o funcionamento interno e a lógica de negócios do aplicativo podem ser revelados. Com essas informações, um atacante pode acessar o banco de dados ou outros recursos de dados. Dependendo dos privilégios da conta obtida a partir do código fonte, pode ser possível ler, atualizar ou excluir dados arbitrários do banco de dados.

A solução para a correção dessa vulnerabilidade consiste em:

a. Confirmar quais aspectos do código-fonte está sendo realmente divulgados.
b. Se for um arquivo exigido pelo aplicativo, alterar suas permissões para impedir que os usuários públicos acessem o mesmo.
c. Certificar-se de que o servidor tenha todos os *patches* de segurança atuais aplicados.
d. Remover todos os arquivos temporários e de backup do servidor da *Web*.

As cidades que apresentaram essas vulnerabilidades foram: Alagoa Grande, Belém, Pocinhos, Santa Rita, São João do Rio do Peixe, Soledade e Uiraúna. Essas vulnerabilidades estão classificadas como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017) e CAPEC (2017).

4.5.4 Cross-site Scripting

Conforme a OWASP (2016) o *Cross-site Scripting* (XSS) refere-se ao ataque de injeção de código do lado do cliente, em que um invasor pode executar *scripts* maliciosos em um site ou aplicativo *web*. Ao executar o XSS, um atacante não tem como alvo uma vítima diretamente. Em vez disso, um invasor explora uma vulnerabilidade dentro de um *site* ou aplicativo da *Web* que a vítima visita, usando essencialmente o site vulnerável como veículo para entregar um *script* malicioso ao navegador da vítima.

O navegador do usuário final entende que o *script* veio de uma fonte confiável, o que permite que esse *script* mal-intencionado possa acessar todos os *cookies*, *tokens* de sessão ou outras informações confidenciais retidos pelo navegador (OWASP, 2016).

Conforme o OWASP (2013), a solução para a correção dessa vulnerabilidade consiste em:

> a. Filtrar adequadamente todos os dados não-confiáveis com base no contexto HTML (corpo, atributo, *JavaScript*, CSS ou URL) no qual os dados serão colocados.
> b. “Lista branca" ou validação de entrada positiva também é recomendada, pois ajuda a proteger contra XSS, mas não é uma defesa completa, já que muitas aplicações requerem caracteres especiais em sua entrada.
> c. Considerar bibliotecas de auto-sanitização como OWASP's AntiSamy ou o Java HTML Sanitizer Project.
> d. Considerar a *Content Security Policy* (CSP) para se defender contra XSS em todo o site. (OWASP, 2013, p. 10).

As cidades que apresentaram essa vulnerabilidade foram: Bananeiras, Lucena e Solânea. Essa vulnerabilidade está classificada como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.5.5 Cifras fracas ativas (tradução livre)

Conforme o iMasters (2016), cifras são um “conjunto de codificações que são especificados por meio de um protocolo de criptografia [...], o tamanho da chave de criptografia [...] e um algoritmo [...] que é usado para verificação da integridade”. A cifra é um algoritmo utilizado no momento em que a informação é criptografada ou descriptografada criando um meio seguro para o transporte da informação pela de Internet.

O Netsparker detectou que cifras fracas são ativadas durante a comunicação segura (SSL). Essas cifras fracas permitem que invasores decifrem o tráfego SSL entre o servidor do município e seus visitantes. Ao contrário, uma cifra forte permite uma criptografia mais eficiente e, portanto, aumenta o esforço necessário para decifrá-la.

Conforme o OWASP (2013), a solução para a correção dessa vulnerabilidade consiste em configurar o servidor *Web* do município para não permitir o uso de cifras fracas.

As cidades que apresentaram essa vulnerabilidade foram: Conde, Guarabira, Itabaiana, João Pessoa, Lagoa Seca, Lucena, Pedras de Fogo, Pocinhos, São João do Rio do Peixe e Uiraúna. Essa vulnerabilidade está classificada como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

4.5.6 Insecure Transportation Security Protocol Supported (SSLv3)

O Netsparker detectou que o protocolo de segurança de transporte inseguro (SSLv3) é suportado pelo servidor *web* do site analisado. Atacantes podem realizar ataques do tipo *man-in-the-middle* e observar o tráfego de criptografia entre o site do município e seus visitantes.

Fornecer proteção de camada de transporte adequada pode afetar o design do site. É mais fácil exigir SSL para todo o site. Por motivos de desempenho, alguns sites usam SSL somente em páginas particulares. Outros usam SSL somente em páginas críticas, mas isso pode expor IDs de sessão e outros dados confidenciais (OWASP, 2010).

Conforme o OWASP (2010), a solução para a correção dessa vulnerabilidade consiste em:

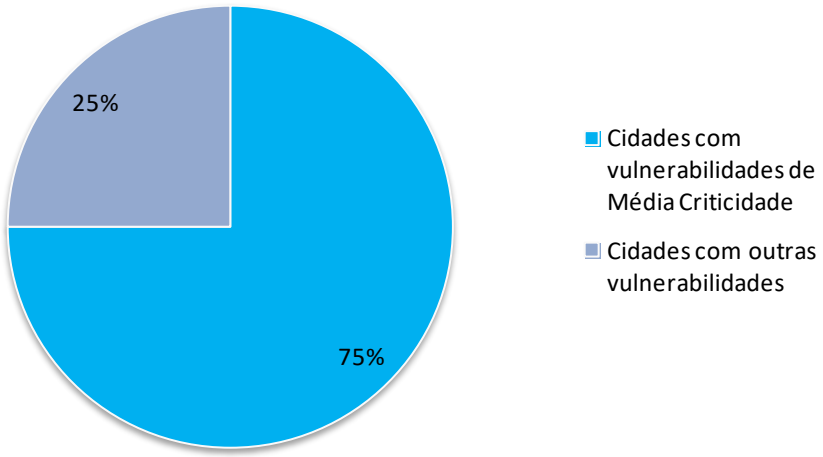
a. Exigir SSL para todas as páginas sensíveis. As solicitações não SSL para essas páginas devem ser redirecionadas para a página SSL.
b. Definir o sinalizador 'seguro' em todos os *cookies* sensíveis.
c. Configurar o provedor de SSL apenas para suportar algoritmos fortes.
d. Certificar-se de que o certificado é válido, não expirado, não revogado e corresponde a todos os domínios usados pelo site.

A cidade que apresentou essa vulnerabilidade foi Pedras de Fogo. Essa vulnerabilidade está classificada como de Média Criticidade em conformidade com as organizações OWASP (2013), PCI (2016), CWE (2017) e CAPEC (2017).

4.6 CONCLUSÃO DO TÓPICO (vulnerabilidades de Baixa Criticidade)

Na varredura foram encontradas 12 tipos de vulnerabilidades de Média Criticidade dentre os portais das cidades analisadas. Ressalta-se que, das 40 cidades participantes da amostra, 30 cidades apresentaram pelo menos uma vulnerabilidade de Média Criticidade (Gráfico 7).

GRÁFICO 7 - Vulnerabilidades de Média Criticidade



Fonte: Dados da pesquisa (2017).

As cidades que apresentaram pelo menos uma vulnerabilidade de Média Criticidade representam 75% da amostra. Dentre as 12 vulnerabilidades de Média Criticidade encontradas pelo software Netsparker, ressaltam-se as vulnerabilidades *Out-of-date Version (jQuery), Weak Ciphers Enabled* e I*nsecure Transportation Security Protocol Supported (SSLv3)* que estiveram presentes em 14, 10 e 7 cidades respectivamente.

A pesquisa realizada pelo iBLISS (2016), que analisou as vulnerabilidades eletrônicas existentes em setores da iniciativa privada, destacou que 49% das vulnerabilidades encontradas no setor privado foram de Média Criticidade. Essa taxa de 49% serve de comparação com a taxa observada para os municípios da Paraíba, analisados nessa pesquisa, que encontrou uma taxa de 75% de vulnerabilidades de Média Criticidade. Novamente, como destaca o *SecurityScorecard R&D Department* (SSD, 2016), as organizações governamentais, quando comparadas à organizações do setor privado, são as que apresentam maior taxa de vulnerabilidades em sua infraestrutura de sistema eletrônico.

Ressalta-se que uma vulnerabilidade de Média Criticidade encontrada na varredura, o C*ross-site Scripting*, está incluída, segundo o relatório da OWASP (2013), entre os dez riscos de segurança mais críticos em aplicações *Web*.

Vulnerabilidades de Média Criticidade não são facilmente exploradas, pois necessita que um atacante utilize de manipulação dos usuários para obter o acesso. Isso não significa que não possa ser explorada, pois um atacante habilidoso, por

meio de várias tentativas conseguiria o acesso indevido e com a possibilidade de gerar prejuízos, inclusive pela descontinuidade do serviço. Sua correção não tem a urgência verificada nos níveis de criticidade “Crítica” e “Alta Criticidade”, mas deve ser corrigida o mais rápido possível.

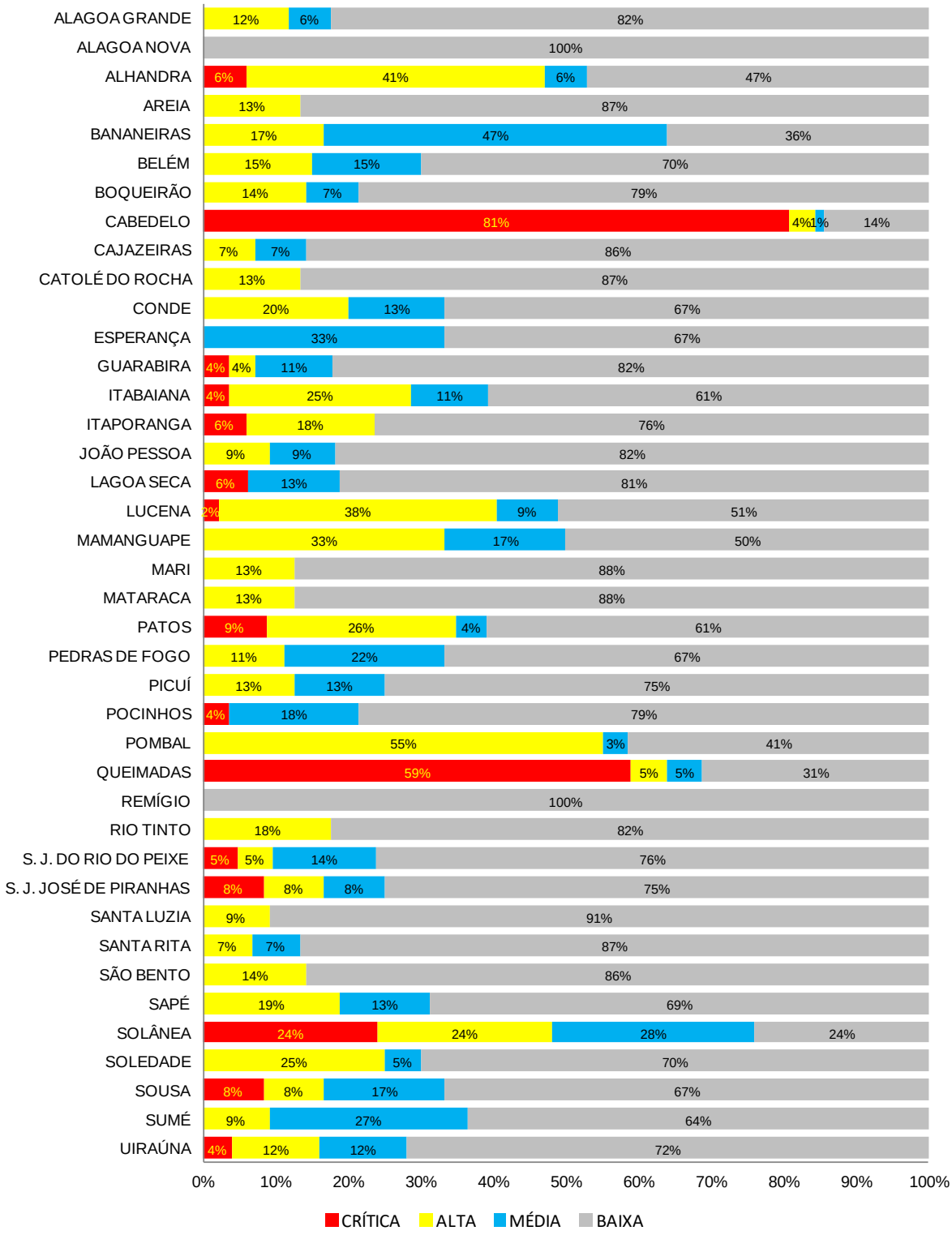
4.7 OUTRAS CONSIDERAÇÕES

Nos tópicos anteriores foram apresentados os resultados encontrados das vulnerabilidades presentes nos portais de governo eletrônico analisados na presente pesquisa. Nesse tópico serão apresentadas algumas considerações gerais sobre os resultados por cidade e como estão dispostas suas vulnerabilidades.

4.7.1 Vulnerabilidades por cidades

A seguir, apresenta-se o gráfico de vulnerabilidades encontradas por cidades e a respectiva distribuição percentual das vulnerabilidades encontradas em cada cidade.

Gráfico 8 - Vulnerabilidades por cidades



Fonte: Dados da pesquisa (2017).

Ressalta-se do Gráfico 8 algumas cidades que apresentaram um alto percentual somado de vulnerabilidades Críticas e de Alta Criticidade, como: Alhandra (47%), Patos (35%), Cabedelo (85%), Lucena (40%), Pombal (55%),

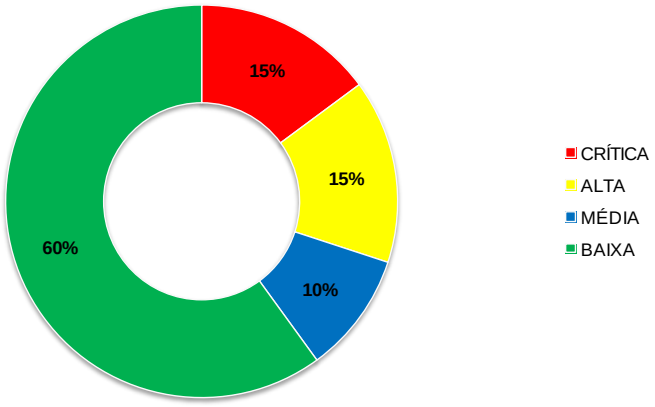
Solânea (48%) e Queimadas (64%). Como comparação, o relatório de ameaças do iBLISS (2016), identificou que em média a soma das vulnerabilidades Críticas e de Alta Criticidade encontradas em setores privados do país, correspondem a 20%, ou seja, alguns municípios possuem um percentual de vulnerabilidades maior que a média do mercado.

Apesar de destacar essas cidades pela alta porcentagem de vulnerabilidades encontradas, não se pode desconsiderar as vulnerabilidades Críticas e de Alta Criticidade encontradas em outras cidades, mesmo com menor percentual. A desatualização de um único software é capaz de comprometer, em larga escala, a segurança dos dados afetando a confiança dos usuários (IBLISS, 2016).

As cidades de Alagoa Nova e Remígio apresentaram apenas vulnerabilidades de Baixa Criticidade. Esse tipo de vulnerabilidade não causa danos significativos à continuidade dos serviços.

O Gráfico 9 mostra o percentual de vulnerabilidade por nível de criticidade, ou seja, o quanto cada vulnerabilidade, por nível de criticidade, representa do total de vulnerabilidades encontradas nos municípios participantes amostra.

Gráfico 9 - Taxa de vulnerabilidades por nível de criticidade



Fonte: Dados da pesquisa (2017).

De acordo com o Gráfico 9, os municípios do Estado da Paraíba, participantes desse estudo, apresentaram 10% de vulnerabilidades de Média Criticidade e 60% de vulnerabilidades de Baixa Criticidade, representando um total de 70% de vulnerabilidades com maior dificuldade de exploração. Ainda assim, as vulnerabilidades de Média Criticidade, se exploradas, podem ter impactos relevantes

e prejudicar os serviços oferecidos pelo portal, bem como expor dados de seus usuários. Para efeito de comparação, o setor privado, conforme o relatório do iBLISS (2016), apresentou 49% e 31% de vulnerabilidades de Média e Baixa Criticidade, respectivamente.

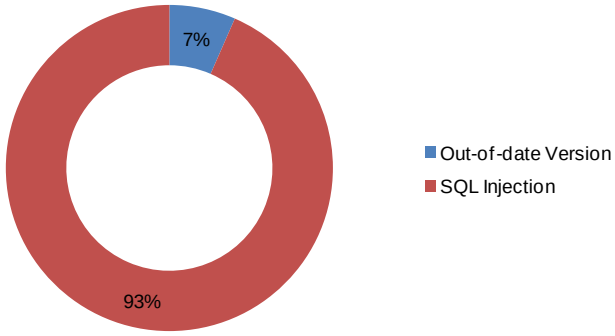
Os municípios analisados apresentaram, em média, uma maior taxa de vulnerabilidades de Baixa Criticidade (60%), em comparação ao setor privado (31%), e, considerando que sempre haverá vulnerabilidades, conhecidas ou não, esse dado pode ser considerado positivo já que esse tipo de vulnerabilidade possui maior dificuldade de exploração e tem menor possibilidade de causar danos significativos à continuidade dos serviços.

Ainda assim, as taxas de vulnerabilidades Críticas (15%) e de Alta Criticidade (15%), representam, juntas, 30% das vulnerabilidades encontradas nos municípios do Estado da Paraíba. Esse é um dado preocupante, pois são vulnerabilidades que necessitam de correção imediata e que são responsáveis pelos mais graves problemas relacionados à violação de dados (IBLISS, 2016).

4.7.2 Vulnerabilidades por nível de criticidade

Nesse tópico apresenta-se o quanto cada tipo de vulnerabilidade encontrada representa por nível de criticidade (Crítica e Alta Criticidade) em que foi destacada. Com isso é possível observar qual tipo de vulnerabilidade acomete mais frequentemente as falhas de segurança dos portais de governo eletrônico dos municípios participantes da amostra. O Gráfico 10 apresenta o tipo de vulnerabilidades Críticas encontradas e o quanto representam pelo nível de criticidade.

Gráfico 10 - Tipo de Vulnerabilidades Críticas

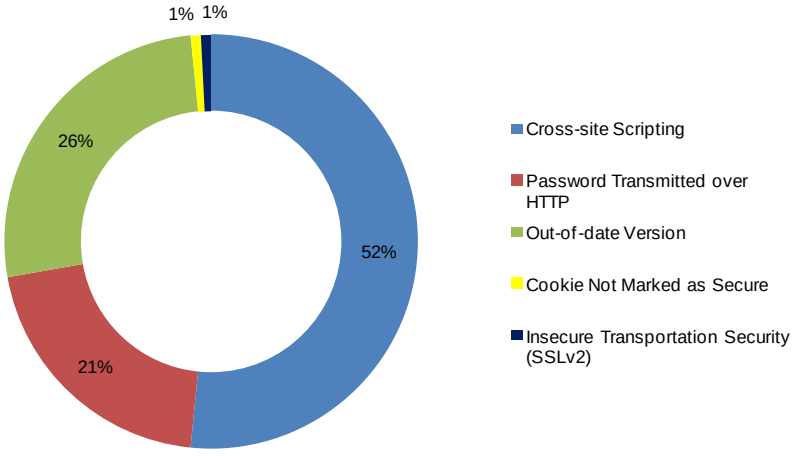


Fonte: Dados da pesquisa (2017).

De acordo com o Gráfico 10, duas vulnerabilidades Críticas foram encontradas sendo a vulnerabilidade *SQL Injection* a que teve maior incidência (93%) nas falhas de segurança. Essa vulnerabilidade é, segundo a OWASP (2013), a que apresenta maiores riscos às organizações, figurando em primeiro lugar entre às dez vulnerabilidades mais críticas encontradas em aplicações *Web*.

O Gráfico 11 apresenta os tipos de vulnerabilidades de Alta Criticidade encontradas nos municípios analisados.

Gráfico 11 - Tipo de vulnerabilidades de Alta Criticidade



Fonte: Dados da pesquisa (2017).

Conforme se observa no Gráfico 11, a vulnerabilidade *Cross-site Scripting* é a que apresenta maior incidência (52%) entre as vulnerabilidades de Alta Criticidade, inserida entre as dez vulnerabilidades mais críticas às aplicações *Web* segundo o relatório da OWASP (2013). Destaca-se, também, a vulnerabilidade *Out of date*

Version (desatualização), que é responsável por 26% das vulnerabilidades de Alta Criticidade, o que evidencia uma dificuldade em gerir eficientemente as atualizações de softwares. Em comparação, o relatório do iBLISS (2016) destacou que as desatualizações de software corresponde a 32% das falhas de segurança do setor privado.

5 CONSIDERAÇÕES FINAIS

A *Internet* tornou-se, tanto um importante local para a busca de informações, quanto um espaço repleto de ameaças eletrônicas, o que leva à necessidade de um maior cuidado em relação à segurança da informação. Os portais de governo eletrônico ao oferecer serviços eletrônicos, por meio da *Internet*, aos diversos interessados, cria um problema substancial para a segurança e a confiança dos cidadãos nos governos. Nesse sentido, essa pesquisa permitiu identificar as vulnerabilidades eletrônicas a que estão sujeitos os portais de governo eletrônico dos municípios do Estado da Paraíba, e que podem comprometer as informações disponibilizadas por seus diversos usuários.

Para isso, identificaram-se os municípios que representavam maior participação econômica no PIB do Estado da Paraíba. Entende-se que, quanto maior a participação econômica de um município e\ou seu desenvolvimento, maior deverá ser seu compromisso em desburocratizar e facilitar o acesso às informações e serviços, para a população, por meio de um portal de governo eletrônico.

Dos 50 municípios identificados para compor a população dessa pesquisa, apenas 40 foram aptos a fazerem parte da amostra para serem analisadas as vulnerabilidades em seus portais de governo eletrônico. Essa foi uma limitação da pesquisa, pois em 10 municípios não foi possível executar o *scanner* de vulnerabilidade em razão de não haver resposta do servidor (computador) responsável por hospedar o portal de governo eletrônico do município.

Essa pesquisa possibilitou obter um panorama das falhas de segurança presentes nos portais de governo eletrônico dos municípios do Estado da Paraíba. Em todos os municípios, os portais analisados apresentaram vulnerabilidades que variaram desde Baixa e Média Criticidade, que não necessitam de correção tão imediata, até vulnerabilidades Críticas e de Alta Criticidade, que necessitam de remediação urgente dada a sua capacidade de interromper a continuação do serviço e comprometer a confidencialidade, integridade e disponibilidade da informação.

Foram encontradas 822 vulnerabilidades nos portais de governo eletrônico dos 40 municípios analisados. Ressalta-se que, 30% dessas 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, pois, essas falhas tem o potencial de causar danos significativos à capacidade dos municípios prestarem serviços aos seus usuários.

Observando a alta taxa de vulnerabilidades Críticas e de Alta Criticidade descobertas nessa pesquisa, pode se inferir a inexistência, ou pelo menos, a ineficiência de uma política de segurança da informação que tenha como um dos objetivos, o monitoramento constante de ameaças eletrônicas a fim de procurar reduzir os impactos negativos de uma possível exploração dessas vulnerabilidades.

Os danos decorrentes da exploração de vulnerabilidades Críticas e de Alta Criticidade permitem o roubo de senhas e de dados sigilosos, acesso remoto, alterações de conteúdo, acesso a dados sigilosos, controle da administração de servidores (computadores), exclusão de dados, etc. Dessa forma, esse estudo contribuiu para a identificação desse tipo de vulnerabilidade, evidenciando as consequências que podem impedir a continuidade dos serviços prestados pela Administração Pública, bem como a possível exposição indevida dos dados de seus usuários, e as possíveis soluções para a correção dessas falhas.

A pesquisa também identificou quais os tipos de vulnerabilidades, por nível de criticidade, mais acometem os portais de governo eletrônico dos municípios do Estado da Paraíba. Essa identificação é importante para saber quais falhas estão mais expostas aos atacantes virtuais, o que permite que uma ação de contingência seja adotada de maneira emergencial para que se reduza a exposição aos ataques e consequentemente diminua seus possíveis danos.

Cabe ressaltar que duas vulnerabilidades identificadas e várias vezes recorrentes na maioria dos municípios analisados foram as *Out-of-Date-Version* (desatualização de *software*) e *Password Transmitted over HTTP* (senha transmitida pelo HTTP). Novamente, infere-se, a partir dessas vulnerabilidades, a falta de uma política básica de segurança da informação e evidencia a fragilidade na questão da segurança da informação em portais de governo eletrônico, pois são duas vulnerabilidades de fácil correção. A desatualização de *software* é facilmente resolvida com um simples cronograma de verificação das possíveis atualizações que são disponibilizadas pelos desenvolvedores dos *softwares* utilizados no desenvolvimento do portal de governo eletrônico. A transmissão não autorizada de senhas pelo HTTP é resolvida alterando o modo de conexão para HTTPS, o que assegura que as informações transmitidas serão criptografadas, aumentando significativamente a segurança dos dados.

Para garantir a segurança da informação de seus portais de governo eletrônico, tanto de rede como da infraestrutura que possibilita o acesso virtual, a Administração Pública, nessa pesquisa representada na figura dos municípios, deve ter uma visão abrangente de seus procedimentos de segurança com a capacidade de avaliar os pontos fortes e fracos em seus sistemas ao longo do tempo.

Com o crescente uso das Tecnologias de Informação e Comunicação, facilitando o processo de interação e integração entre governos e usuários, a Administração Pública se utiliza dos portais de governo eletrônico não apenas para a disponibilização de informações e serviços, mas também como meio de evidenciar, de maneira transparente, suas atividades e, consequentemente, diminuir a burocracia.

A interação e integração entre governo e usuários levam à necessidade de retenção de dados destes usuários, logo, isto passa a ser um ponto crucial na administração de um sistema de governo eletrônico, pois a responsabilidade por garantir a segurança dessas informações, torna-se um desafio para os governos. Essas informações precisam de ferramentas de proteção robustas, tanto em sistemas quanto em infraestrutura, como também de políticas que adotem as boas práticas de segurança e que sigam os padrões e normas vigentes, a fim de impedir que o acesso não autorizado possa comprometer ou prejudicar a continuidade dos serviços do governo ou divulgar a privacidade dos dados dos cidadãos.

Antes da implantação de um sistema de governo eletrônico os municípios deveriam ter como prioridade a segurança dessa aplicação, eliminando, ou pelo menos diminuindo, as falhas que possam ocorrer na rede e no desenvolvimento dos portais. Conforme análise dos dados, essa prioridade com a segurança parece não ter ocorrido, pois 95% municípios participantes da amostra, apresentaram vulnerabilidades com o potencial de prejudicar a continuidade dos serviços e/ou expor os dados de seus usuários. Infere-se, desse dado, que existe a necessidade de monitoramento constante por parte dos desenvolvedores desse sistema na busca de vulnerabilidades e no aperfeiçoamento da segurança.

É possível concluir, por meio dos resultados, que a segurança das informações dispostas nos portais de governo eletrônico dos municípios do Estado da Paraíba, não está adequadamente protegida, tanto por falha no desenvolvimento do sistema, quanto por falta de uma política de segurança. Esse resultado corrobora com o relatório apresentado pelo TCU (2014) no qual identificou que 61% das

organizações da Administração Pública Federal não apresentam capacidade adequada de Governança e Gestão de TI, ou seja, não conseguem gerir de forma eficaz a proteção das informações que contribuem para que os objetivos das organizações sejam atingidos.

Ameaças eletrônicas estão em constante desenvolvimento e sempre em busca de vulnerabilidades que permitam o acesso às informações sigilosas de usuários. Observa-se que os portais de governo eletrônico, dos municípios estudados, não estão suficientemente protegidos para evitar consistentemente essas ameaças. É necessário um constante gerenciamento da segurança desses portais, verificando as vulnerabilidades e fraquezas do sistema.

Por fim, é imprescindível a adoção de uma política de segurança que acompanhe e monitore cada etapa de implantação do sistema de governo eletrônico, a fim de minimizar as vulnerabilidades decorrentes de falhas de programação e as possibilidades de sua exploração. O estudo traz um alerta aos gestores dos portais analisados, pois independente do nível de criticidade das vulnerabilidades identificadas, todos os participantes da amostra apresentaram algum tipo de falha em seus portais. Os administradores públicos devem considerar o uso de ferramentas de detecção de vulnerabilidades para ajudar a examinar e desenvolver planos que solucionem os problemas em curto e longo prazo.

REFERÊNCIAS

ACUNETIX. **Why is Source Code Disclosure dangerous?** Disponível em <https://www.acunetix.com/blog/articles/source-code-disclosure-dangerous/>. Acesso em 16 abr. 2017.

AKMAN, Ibrahim *et al*. E-Government: A global view and an empirical evaluation of some attributes of citizens. **Government Information Quarterly**, v. 22, n. 2, p. 239-257, 2005.

ALEXANDER, Dawn; GILES, April. Protecting web sites. In: BIDGOLI, Hossein. **Handbook of information security**: threats, vulnerabilities, preventions, detection, and management. New Jersey: Wiley, 2006. v. 3, p. 370-378.

ALMARABEH, Tamara; ABUALI, Amer. A general framework for e-government: definition maturity challenges, opportunities, and success. **European Journal of Scientific Research**, v. 39, n. 1, p. 29-42, 2010.

AQUINO, Mirian de Albuquerque. Ciência e método: elementos para reflexão nas pesquisas em ciência da informação.In: AQUINO, Mirian de Albuquerque; OLIVEIRA, Henry Poncio Cruz; LIMA, Izabel França (Org.). **Experiências metodológicas em ciência da informação**. Brasília: 2013. p. 19-47.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2008**. Tecnologia da Informação – técnicas de segurança – gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013**. Tecnologia da Informação – técnicas de segurança – código de prática para controles de segurança da informação. 2. ed. Rio de Janeiro, 2013.

AUSTRALIAN CYBER SECURITY CENTRE THREAT. **Threat Report**: 2015. [S.l.: s.n], 2015. Disponível em: <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf>. Acesso em: 16 out. 2016.

BANCO MUNDIAL. **e-Goverment**. 2015. Disponível em: <http://www.worldbank.org/en/topic/ict/brief/e-government.> Acesso em: 13 jul. 2016.

BORDER, Charles. Client-side security. In: BIDGOLI, Hossein. **Handbook of information security**: threats, vulnerabilities, preventions, detection, and management. New Jersey: Wiley, 2006. v. 3, p. 342-354.

BRASIL. Presidência da República. **Plano Diretor da Reforma do Aparelho do Estado.** Brasília, novembro 1995. 68 p. Disponível em: <http://www.cebes.org.br/media/File/Plano%20Diretor%20da%20Reforma%20do%20Aparelho%20do%20Estado.pdf>. Acesso em: 13 jul. 2016.

BRASIL. Decreto de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 19 out. 2000a.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Proposta de Política de Governo Eletrônico para o Poder Executivo Federal**. Grupo de Trabalho "Novas Formas Eletrônicas de Interação". Brasília: Ministério do Planejamento, Orçamento e Gestão, 2000b.

BRASIL. Decreto n.º 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**, Brasília, DF, 14 jun. 2000c. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm >. Acesso em: 14 out. 2016.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. (Comitê Executivo do Governo Eletrônico). **2 Anos de Governo Eletrônico.** Balanço de Realizações e Desafios Futuros. Brasília: DF, 2002, 46 p. Disponível em: <http://www.governoeletronico.gov.br/documentos-e-arquivos/E15_90balanco_2anos_egov.pdf>. Acesso em: 22 set. 2016.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa n. 1, de 13 de junho de 2008. **Diário Oficial da União**, Brasília, DF, 18 jun. 2008a.

BRASIL. Tribunal de Contas da União. **Acórdão nº 1.603/2008.** 2008b. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 13/08/2008. Disponível em: <http://www.mp.go.gov.br/portalweb/hp/12/docs/acordao_tcu_-_13-08-2008.pdf>. Acesso em: 25 out. 2016.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 4. ed. Brasília, DF, 2012.

BRASIL. Tribunal de Contas da União. **Acórdão nº 2.308/2010.** 2010. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 8/9/2010. Disponível em: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14D78C1F1014D794CB1636774>. Acesso em: 25 out. 2016.

BRASIL. Tribunal de Contas da União. **Acórdão nº 3.117/2014.** 2014. Plenário. Relator: Ministro Augusto Sherman Cavalcanti. Sessão de 12/11/2014. Disponível em: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14D78C1F1014D794C57073235>. Acesso em: 25 out. 2016.

BRASIL. Decreto nº. 8.638, de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. **Diário Oficial da União**, Brasília, DF, 18 jan. 2016a.

BRASIL. Decreto nº. 8.818, de 21 de julho de 2016. **Diário Oficial da União**, Brasília, DF, 22 jul. 2016b.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Estratégia de Governança Digital da Administração Pública Federal 2016-19.** Brasília: DF, 2016c. Disponível em: <http://www.governoeletronico.gov.br/egd/estrategia-de-governanca-digital>. Acesso em: 22 set. 2016.

BURN, Janice; ROBINS, Greg. Moving towards e-government: a case study of organisational change processes. **Logistics Information Management**, v. 16, n. 1, p. 25-35, 2003.

CALDAS, Luiz Carlos Agner. **Arquitetura de informação e governo eletrônico**: diálogo cidadãos-estado na world wide web: estudo de caso e avaliação ergonômica de usabilidade de interfaces humano-computador. 2007. 353 f. Tese (Doutorado em Artes de Design) – Pontifícia Universidade Católica, Rio de Janeiro, 2007.

CAPURRO, Rafael; HJØRLAND, Birger. The concept of information. **Annual Review of Information Science and Technology**, v. 37, n. 1, p. 343-411, 2003.

CARVALHO, Paulo Sérgio Melo. Conferência de abertura: o setor cibernético nas forças armadas brasileiras. In: BARROS, Otávio Santana Rego; GOMES, Ulisses Mesquita (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: 2011. p. 13-34. Disponível em: <http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf >. Acesso em: 14 out. 2016.

CENTER FOR DEMOCRACY & TECHNOLOGY. T**he e-government handbook for developing countries**. [S.l.: s.n], 2002. Disponível em: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN007462.pdf >. Acesso em: 14 set. 2016.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **Net Losses:** Estimating the Global Cost of Cybercrime. [S.l.: s.n], 2014. Disponível em: <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>. Acesso em: 16 out. 2016.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet.** São Paulo, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 01 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 1° trimestre. 2015. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_1o_Trimestre_2015.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 2° trimestre. 2015. Disponível em:

<http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_2o_Trimestre_2015.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 3° trimestre. 2015. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_3o_Trimestre_2015.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 4° trimestre. 2015. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_4o_Trimestre_2015.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 1° trimestre. 2016. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2016/Estatisticas_CTIR_Gov_1o_Trimestre_2016.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 2° trimestre. 2016. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2016/Estatisticas_CTIR_Gov_2o_Trimestre_2016.pdf>. Acesso em: 15 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede do ano de 2015**. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_Ano_2015.pdf>. Acesso em: 15 out. 2016.

CHOO, Kim-Kwang Raymond. The cyber threat landscape: Challenges and future research directions. **Computers & Security**, v. 30, n. 8, p. 719-731, 2011.

COMITÊ GESTOR DA INTERNET. **TIC governo eletrônico 2013: pesquisa sobre o uso das tecnologias da informação e comunicação no setor público brasileiro**. São Paulo: Comitê Gestor da Internet no Brasil, 2014. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2013_LIVRO_ELETRONICO.pdf>. Acesso em: 17 jul. 2016.

COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION. Disponível em: <https://capec.mitre.org/>. Acesso em: 13 abr. 2017.

COMMON WEAKNESS ENUMERATION**. Cross-site Scripting.** Disponível em: <https://cwe.mitre.org/data/definitions/79.html>. Acesso em: 13 abr. 2017.

DAMIAN, Ieda Pelógia Martins; MERLO, Edgard Monforte. Uma análise dos sites de governos eletrônicos no Brasil sob a ótica dos usuários dos serviços e sua satisfação. **Revista de Administração Pública**, v. 47, n. 4, p. 877-900, 2013.

DANTAS, Marcos Leal. **Segurança da Informação:** uma abordagem focada em gestão de riscos**.** Olinda: Elógica, 2011. cap. 1, p. 9-40.

DINIZ, Eduardo Henrique et al. O governo eletrônico no Brasil: perspectiva histórica a partir de um modelo estruturado de análise. **Revista de Administração Pública**, v. 43, n. 1, p. 23-48, 2009.

DITTRICH, David; HIMMA, Kenneth Einar. Active Response to Computer Intrusions. In: BIDGOLI, Hossein. **Handbook of information security**: threats, vulnerabilities, preventions, detection, and management. New Jersey: Wiley, 2006. v. 3, p. 664-680.
EBRAHIM, Zakareya; IRANI, Zahir. E-government adoption: architecture and barriers. **Business process management journal**, v. 11, n. 5, p. 589-611, 2005.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **ENISA Threat Landscape 2015**. [S.l.: s.n], 2016. Disponível em: <https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport>. Acesso em: 16 out. 2016.

FANG, Zhiyuan. E-government in digital era: concept, practice, and development. **International journal of the Computer, the Internet and management**, v. 10, n. 2, p. 1-22, 2002.

FREIRE, Felipe Ribeiro; STABILE, Max. As novas tecnologias e a participação eletrônica: entre promessas e desafios. In: BARBOSA, Alexandre F. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e comunicação no setor público brasileiro:** TIC governo eletrônico 2013. São Paulo: 2014. p. 47-56. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2013_LIVRO_ELETRONICO.pdf>. Acesso em: 25 ago. 2016.

G1.GLOBO.COM. **Hackers da Sony ameaçam cinemas que exibirem filme 'A entrevista**. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/12/hackers-da-sony-ameacam-cinemas-que-exibirem-filme-entrevista.html>. Acesso em: 24 out. 2016.

GARCIA, Rodrigo Moreira. Governo eletrônico, informação e competência em informação. **Informação & Sociedade**, v. 16, n. 2, 2006. p. 79-87.

GOVERNMENT ACCOUNTABILITY OFFICE - GAO. **Information Security:** Cyber Threats and Vulnerabilities Place Federal Systems at Risk. [S.l.: s.n], 2009. Disponível em: <http://www.gao.gov/assets/130/122454.pdf>. Acesso em: 16 out. 2016.

GOVERNMENT ACCOUNTABILITY OFFICE - GAO. **Information Security:** federal agencies need to better protect sensitive data. [S.l.: s.n], 2015. Disponível em: <http://www.gao.gov/assets/680/673678.pdf>. Acesso em: 16 out. 2016.

GRÖNLUND, Åke. State of the art in e-Gov research–a survey. In: **International Conference on Electronic Government**. Springer Berlin Heidelberg, 2004. p. 178-185.

GUPTA, Babita; DASGUPTA, Subhasish; GUPTA, Atul. Adoption of ICT in a government organization in a developing country: An empirical study. **Journal of Strategic Information Systems**, v. 17, p. 140-154, 2008.

IBLISS. **Relatório de Ameaças de 2016**. Disponível em: <https://www.ibliss.com.br/relatorio-de-ameacas-2016/>. Acesso em: 5 mar. 2017.

IBRAHIM, Omar Ahmed; ZAKARIA, Nor Hidayati. Towards the Development of an Adoption Model for E-Government Services in Developing Countries. 2015. Disponível em: <http://pacis2015.comp.nus.edu.sg/_proceedings/PACIS_2015_submission_345.pd> Acesso em: 12 jul. 2016.

IMASTER. **Monitorar a segurança do SSL é possível?** Disponível em: <https://imasters.com.br/infra/seguranca/monitorar-seguranca-do-ssl-e-possivel/?trace=1519021197&source=single>. Acesso em: 16 abr. 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. Disponível em: <http://cidades.ibge.gov.br/download/mapa_e_municipios.php?lang=&uf=pb>. Acesso em 27 de out. 2016.

INSTITUTO DE DESENVOLVIMENTO MUNICIPAL E ESTADUAL. **Anuário 2014**. Disponível em: <http://ideme.pb.gov.br/servicos/anuarios-online/anuario-2014.pdf/view>. Acesso em: 27 de out. 2016.

INTERNATIONAL STANDARDS ORGANIZATION - ISO. **ISO/IEC 27000**: Information technology - Security techniques - Information security management systems - Overview and Vocabulary. 3. ed. Switzerland, 2014.

JUNIPER RESEARCH. **Cybercrime will cost businesses over $2 trillion by 2019.** 2015. Disponível em: <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>. Acesso em: 16 out. 2016.

KENNEDY, Aileen; COUGHLAN, Joseph P.; KELLEHER, Carol. Business process change in e-government projects: the case of the Irish land registry.**Technology Enabled Transformation of the Public Sector:** Advances in E-Government: Advances in E-Government. 2012.

KOCHANOVA, Anna; HASNAIN, Zahid; LARSON, Bradley. Does e-government improve government capacity? evidence from tax administration and public procurement. Evidence from Tax Administration and Public Procurement. **World Bank Policy Research Working Paper**, n. 7657, p.1-31, 2016.

MANDARINO JÚNIOR, Raphael; CANONGIA, Cláudia. **Segurança cibernética no Brasil:** livro verde. Gabinete de Segurança Institucional (GSI), Brasília, DF, 2010.

MANTOVANE, Solange Aparecida. **A política de governo eletrônico no Brasil:** uma análise dos governos FHC e Lula. 2012. 92 f. Dissertação (Mestrado em Ciência Política) – Universidade Federal de São Carlos, São Paulo.

MEDEIROS, Paulo Henrique Ramos. **Governo eletrônico no Brasil**: aspectos institucionais e reflexos na governança. 2004. 314 f. Dissertação (Mestrado em Administração) - Universidade de Brasília, Brasília-DF.

MEDEIROS*,* Paulo Henrique Ramos; GUIMARÃES , Tomás de Aquino. O estágio do governo eletrônico no Brasil em relação ao contexto mundial. **Revista do Serviço Público**, v. 55, n. 1-2, 2004. Disponível em: <http://seer.enap.gov.br/index.php/RSP/article/view/245/250>. Acesso em: 12 set. 2016.

MERKOW, Mark S. E-Commerce safeguards. In: BIDGOLI, Hossein. **Handbook of information security**: threats, vulnerabilities, preventions, detection, and management. New Jersey: Wiley, 2006. v. 3, p. 552-561.

MICHEL, Maria Helena. **Metodologia e pesquisa científica em ciências sociais:** um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos. 3. ed. São Paulo: Atlas, 2015.

NATIONAL VULNERABILITY DATABASE. **Statistics:** Raw Data. [S.l.: s.n], 2016. Disponível em: <https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&cvss_version=3>. Acesso em: 17 out. 2016.

NORRIS, Donald F.; REDDICK, Christopher G. Local e-government in the United States: Transformation or incremental change?. **Public Administration Review**, v. 73, n. 1, p. 165-175, 2013.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **CERT.br aponta aumento de notificações de ataques a servidores Web**. 2016. Disponível em: <http://www.nic.br/noticia/releases/cert-br-aponta-aumento-de-notificacoes-de-ataques-a-servidores-web/>. Acesso em: 29 set. 2016.

OLHAR DIGITAL. **Hackers invadem site da NASA em nome do Brasil**. 2013. Disponível em: <http://olhardigital.uol.com.br/fique_seguro/noticia/hackers-invadem-site-da-nasa-em-nome-do-brasil/37428>. Acesso em: 24 out. 2016.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OECD. **The case of E-government**: Excerpts from the OECD Report “The E-Government Imperative”. Paris: OECD, 2003. Disponível em: <https://www.oecd.org/gov/budgeting/43496369.pdf>. Acesso em: 23 de jun. 2016.

OPEN WEB APPLICATION SECURITY PROJECT. **Cross-site Scripting (XSS)**. Disponível em: <https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)>. Acesso em: 13 abr. 2017.

OPEN WEB APPLICATION SECURITY PROJECT. **Insufficient Transport Layer Protection (2010).** Disponível em: <https://www.owasp.org/index.php/Top_10_2010-A9-Insufficient_Transport_Layer_Protection>. Acesso em: 15 abr. 2017.

OPEN WEB APPLICATION SECURITY PROJECT. **Owasp Top 10-2013**: the ten most critical web application security risks. 2013. Disponível em: <http://www.lulu.com/shop/owasp-foundation/owasp-top-10-2013/paperback/product-21241952.html>. Acesso em: 26 de out. 2016.

PAYMENT CARD INDUSTRY. **The prioritized approach to pursue PCI DSS compliance.** Disponível em: <https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf?agreement=true&time=1493141839795>. Acesso em: 13 abr. 2017.

PEREIRA, Luiz Carlos Bresser. Reflexões sobre a reforma gerencial brasileira de 1995. **Revista do Serviço Público**, v. 50, n. 4, p. 5-29, 1999.

PINHEIRO, Patrícia Peck. **Guerra digital e cyberterrorismo**. 2015. Disponível em: <http://www.brasilpost.com.br/patricia-peck-pinheiro/guerra-digital-e-cyberter_b_6611486.html>. Acesso em: 24 out. 2016.

PINHO, José Antônio Gomes. Investigando portais de governo eletrônico de estados no Brasil: muita tecnologia, pouca democracia. **Revista de Administração Pública**, v. 42, n. 3, p. 471-493, 2008.

PONEMON INSTITUTE. **2015 Cost of Cyber Crime Study:** Brazil. [S.l.: s.n], 2015a. Disponível em: <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-1889ptl.pdf>. Acesso em: 16 out. 2016.

PONEMON INSTITUTE. **2015 Cost of Cyber Crime Study:** Global. [S.l.: s.n], 2015. Disponível em: <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-1889ptl.pdf>. Acesso em: 16 out. 2016.

PRADO, Otávio. **Governo eletrônico, reforma do estado e transparência:** o programa de governo eletrônico do Brasil. 2009. 197 f. Tese (Doutorado em Administração Pública e Governo) - Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2009.

PRADO, Otávio; RIBEIRO; Manuella Maia; DINIZ, Eduardo. Governo eletrônico e transparência: olhar crítico sobre os portais do governo federal brasileiro. In: PINHO, José Antonio Gomes (Org.). **Estado, sociedade e interações digitais:** expectativas democráticas. Salvador: Edfufba, 2012. p. 15-41. Disponível em: <https://repositorio.ufba.br/ri/bitstream/ri/16738/3/estado%2c%20sociedade%20e%20interacoes.pdf>.

RAMINELLI, Francieli Puntel; RODEGHERI; Letícia Bodanese; OLIVEIRA, Rafael Santos. A lei brasileira de acesso à informação no governo eletrônico e sua utilização pelo poder executivo municipal: uma análise do portal da prefeitura de Santa Maria – RS. In: ROVER, Aires José; SANTOS, Paloma Maria; MEZZAROBA, Orides (Org.). **Governo Eletrônico e Inclusão Digital**. Florianópolis: Conceito Editorial 2014. p. 134-156. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/livro_governo_eletronico_e_inclusao_digital_final_0.pdf>. Acesso em: 29 ago. 2016.

RAMOS, Albenides. **Metodologia da pesquisa**: como uma monografia pode abrir o horizonte do conhecimento. São Paulo: Atlas, 2009.

RAUPP, Mauri Fabiano; BEUREN, Ilse Maria. Metodologia de Pesquisa Aplicável as Ciências Sociais. In: BEUREN, Ilse Maria. **Como elaborar trabalhos monográficos em contabilidade**: teoria e prática. 2.ed. São Paulo: Altas, 2004.

RIBEIRO, Sérgio Luís. Estratégia de proteção da infraestrutura crítica de informação e defesa cibernética nacional. In: BARROS, Otávio Santana Rego; GOMES, Ulisses Mesquita (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: 2011. p. 145-163. Disponível em: <http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf >. Acesso em: 24 out. 2016.

SANTOS, Ernani Marques; REINHARD, Nicolau. Disponibilização e uso de serviços de governo eletrônico no Brasil: a visão dos usuários. In: PINHO, José Antônio Gomes (Org.). **Estado, sociedade e interações digitais: expectativas democráticas**. Salvador: Edufba, 2012. p. 121-136.

SECURITYSCORECARD R&D DEPARTMENT. **Government Cybersecurity Report 2016**. Disponível em: <https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf>. Acesso em: 15 abr. 2017

SILCOCK, Rachel. What is e-government. **Parliamentary affairs**, v. 54, n. 1, p. 88-101, 2001.

SILVA, Otávio Carlos Cunha. A segurança e as ameaças cibernéticas: uma visão holística. In: BARROS, Otávio Santana Rego; GOMES, Ulisses Mesquita (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: 2011. Disponível em: <http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf >. Acesso em: 14 out. 2016.

SILVA, Rodrigo Cardoso. **Governo eletrônico nos Estados federados brasileiros**. 2013. 139 f. Dissertação (Mestrado em Direito) – Universidade Católica de Santos, Santos-SP.

SINGH, Saroj Kumar; PARIHAR, Ankita. E-government in India: opportunities and challenges. **Advanced Research in Electrical and Electronic Engineering**, v. 2, n. 14, p. 13-16, 2015.

SLADE, Border. Computer Viruses and Worms. In: BIDGOLI, Hossein. **Handbook of information security**: threats, vulnerabilities, preventions, detection, and management. New Jersey: Wiley, 2006. v. 3, p. 94-106.

SULTAN, Abobakr; AIAFARJ, A. Khalid; ALKUTBI, Ghassan A. Analytic hierarchy process for the success of e-government. **Business Strategy Series**, v. 13, n. 6, p. 295-306, 2012.

SYMANTEC. **ISTR**: Internet Security Threat Report 2016. [S.l.: s.n], 2016. Disponível em: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>. Acesso em: 16 out. 2016.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil:** livro verde. Ministério da Ciência e Tecnologia (MCT), Brasília, DF, 2000.

TECMUNDO. **Hacker russo invade sistema de uma estação de tratamento de água de Springfield**. 2011. Disponível em:<http://www.tecmundo.com.br/ataque-hacker/15631-hacker-russo-invade-sistema-de-uma-estacao-de-tratamento-de-agua-de-springfield.htm>. Acesso em: 24 out. 2016.

TEO, Thompson SH; SRIVASTAVA, Shirish C.; JIANG, Li. Trust and electronic government success: An empirical study. **Journal of management information systems**, v. 25, n. 3, p. 99-132, 2008.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **The use of the internet for terrorist purposes**. [S.l.: s.n], 2012. Disponível em: <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>. Acesso em: 18 out. 2016.

UNITED NATIONS. E-Government Survey 2014: E-Government for the future we want. **United Nations Department of economic and social affairs**, 2014. Disponível em: <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf>. Acesso em: 15 jul. 2016.

UTO, Nelson. **Teste de invasão de aplicações web.** Rio de Janeiro, 2013, Disponível em: <https://esr.rnp.br/livro/seg9#p/20>. Acesso em: 25 de out. 2016.

VAN DER MEULEN, Nicole; JO, Eun A.; SOESANTO, Stefan. **Cybersecurity in the European Union and Beyond**: Exploring the Threats and Policy Responses. Brussels: Policy Departament, 2015.

WEB APPLICATION SECURITY CONSORTIUM. Disponível em: <http://www.webappsec.org/>. Acesso em: 13 abr. 2017.

WEERAKKODY, Vishanth; DHILLON, Gurjit. Moving from e-government to t-government: a study of process reengineering challenges in a UK local authority context. **International Journal of Electronic Government Research**, v. 4, n. 4, p. 1, 2008.

WEST, Darrell M. E-government and the transformation of service delivery and citizen attitudes. **Public administration review**, v. 64, n. 1, p. 15-27, 2004.

WHITMAN, Michael E; MATTORD, Herbert J. **Principles of information security.** 4. ed. Boston: Cengage, 2011.

YILDIZ, Mete. E-government research: Reviewing the literature, limitations, and ways forward.**Government Information Quarterly**, v. 24, n. 3, p. 646-665, 2007.

ZAP. **Mega ataque pirata causou sexta-feira negra para gigantes da internet.** 2016. Disponível em: <http://zap.aeiou.pt/mega-ataque-pirata-deitou-abaixo-twitter-xbox-live-psn-e-spotify-135061>. Acesso em: 24 out. 2016.

ZUCCARO, Paulo Martino. Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: BARROS, Otávio Santana Rego; GOMES, Ulisses Mesquita (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: 2011. p. 49-77. Disponível em: <http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf >. Acesso em: 19 out. 2016.

APENDICE A – Vulnerabilidades de Baixa Criticidade

		MUNICÍPIOS							
VULNERABILIDADE	CRITICIDADE	Alagoa Grande	Alagoa Nova	Alhandra	Areia	Bananeiras	Belém	Boqueirão	Cabedelo
Internal Server Error	Baixa			x		x			x
Autocomplete Enabled	Baixa	x		x	x	x	x	x	x
Cookie Not Marked as HttpOnly	Baixa	x			x	x	x	x	x
Database Error Message Disclosure	Baixa								x
Programming Error Message	Baixa								x
Version Disclosure (PHP)	Baixa	x			x	x	x		
Version Disclosure (ASP.NET)	Baixa								x
Programming Error Message	Baixa	x			x	x	x	x	
Insecure Frame (External)	Baixa	x		x	x	x	x	x	x
Missing X-Frame-Options Header	Baixa	x	x	x	x	x	x	x	x
Missing Content-Type Header	Baixa	x			x	x	x		x
Insecure Transportation Security Protocol Supported (TLS 1.0)	Baixa	x		x	x	x	x	x	
[Possible] Cross-site Request Forgery	Baixa	x		x	x		x		x
[Possible] Cross-site Request Forgery in Login Form	Baixa	x		x	x	x	x		x
[Possible] Phishing by Navigating Browser Tabs	Baixa								x
Misconfigured Access-Control-Allow-Origin Header	Baixa	x			x	x	x		
Mixed Content over HTTPS	Baixa	x			x	x	x		
[Possible] Phishing by Navigating Browser Tabs	Baixa	x		x	x	x	x	x	
.DS_Store File Found	Baixa						x		

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		Cajazeiras	Catolé	Conde	Esperança	Guarabira	Itabaiana	Itaporanga	João Pessoa
Internal Server Error	Baixa	x		x		x	x		
Autocomplete Enabled	Baixa	x	x	x				x	x
Cookie Not Marked as HttpOnly	Baixa	x	x	x		x		x	x
Database Error Message Disclosure	Baixa		x					x	
Programming Error Message	Baixa	x				x			
Out-of-date Version (Apache)	Baixa					x			
Version Disclosure (PHP)	Baixa		x			x	x	x	x
Version Disclosure (Apache)	Baixa			x		x			
Version Disclosure (OpenSSL)	Baixa					x			
Version Disclosure (Apache Module)	Baixa					x			
Version Disclosure (mod_ssl)	Baixa					x			
Version Disclosure (Apache Coyote)	Baixa								x
Apache MultiViews Enabled	Baixa								x
Insecure Frame (External)	Baixa	x	x	x		x	x	x	x
Missing X-Frame-Options Header	Baixa	x	x	x	x	x	x	x	x
Missing Content-Type Header	Baixa						x		
Insecure Transportation Security Protocol Supported (TLS 1.0)	Baixa	x	x	x	x	x	x	x	x
Windows Username Disclosure	Baixa			x					
[Possible] Internal IP Address Disclosure	Baixa	x	x		x			x	
[Possible] Cross-site Request Forgery	Baixa	x	x	x		x	x	x	
[Possible] Cross-site Request Forgery in Login Form	Baixa	x	x	x				x	
[Possible] Phishing by Navigating Browser Tabs	Baixa		x				x		x
Misconfigured Access-Control-Allow-Origin Header	Baixa	x				x			
Mixed Content over HTTPS	Baixa		x		x	x	x	x	

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		Lagoa Seca	Lucena	Mamanguape	Mari	Mataraca	Patos	Pedras de Fogo	Picuí
Internal Server Error	Baixa				x	x		x	
Autocomplete Enabled	Baixa			x	x	x	x	x	
Cookie Not Marked as HttpOnly	Baixa			x	x	x	x	x	
Database Error Message Disclosure	Baixa			x			x		
Programming Error Message	Baixa			x	x	x			
Out-of-date Version (Apache)	Baixa	x	x						
Version Disclosure (PHP)	Baixa		x		x	x	x	x	x
Version Disclosure (Apache)	Baixa	x	x						
Version Disclosure (OpenSSL)	Baixa	x	x						
Version Disclosure (Apache Module)	Baixa	x	x						
Version Disclosure (mod_ssl)	Baixa	x	x						
Version Disclosure (Python)	Baixa		x						
Programming Error Message	Baixa		x				x		
Insecure Frame (External)	Baixa	x	x	x	x	x	x	x	x
Missing X-Frame-Options Header	Baixa	x	x	x	x	x	x	x	x
Missing Content-Type Header	Baixa				x	x		x	
Insecure Transportation Security Protocol Supported (TLS 1.0)	Baixa	x	x	x	x	x	x	x	x
[Possible] Internal IP Address Disclosure	Baixa						x		
[Possible] Cross-site Request Forgery	Baixa		x	x	x	x	x	x	x
[Possible] Cross-site Request Forgery in Login Form	Baixa			x	x	x	x	x	
[Possible] Phishing by Navigating Browser Tabs	Baixa		x		x	x			x
Misconfigured Access-Control-Allow-Origin Header	Baixa			x	x	x		x	
Mixed Content over HTTPS	Baixa		x	x	x	x	x		
[Possible] Phishing by Navigating Browser Tabs	Baixa			x			x	x	
[Possible] Backup File Disclosure	Baixa						x		

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		Pocinhos	Pombal	Queimadas	Remigio	Rio Tinto	Santa Luzia	Santa Rita	São Bento
Internal Server Error	Baixa		x			x	x	x	
Autocomplete Enabled	Baixa		x			x		x	x
Cookie Not Marked as HttpOnly	Baixa		x	x		x	x	x	x
Database Error Message Disclosure	Baixa								
Programming Error Message	Baixa		x	x		x		x	x
Out-of-date Version (Apache)	Baixa	x							
Out-of-date Version (Nginx)	Baixa								
Version Disclosure (PHP)	Baixa	x		x		x		x	x
Version Disclosure (Apache)	Baixa	x					x		
Version Disclosure (OpenSSL)	Baixa	x							
Version Disclosure (Apache Module)	Baixa	x							
Version Disclosure (mod_ssl)	Baixa	x							
Insecure Frame (External)	Baixa	x	x	x	x	x	x	x	x
Missing X-Frame-Options Header	Baixa	x	x	x	x	x	x	x	x
Missing Content-Type Header	Baixa					x		x	x
Windows Short Filename	Baixa						x		
Insecure Transportation Security Protocol Supported (TLS 1.0)	Baixa	x	x	x	x	x		x	x
[Possible] Internal IP Address Disclosure	Baixa		x		x				
[Possible] Cross-site Request Forgery	Baixa	x	x	x		x	x	x	
[Possible] Cross-site Request Forgery in Login Form	Baixa					x	x	x	x
[Possible] Phishing by Navigating Browser Tabs	Baixa	x	x	x		x			
Misconfigured Access-Control-Allow-Origin Header	Baixa					x	x	x	x
Mixed Content over HTTPS	Baixa	x	x	x	x	x			x
[Possible] Phishing by Navigating Browser Tabs	Baixa				x		x	x	x

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		São João do Rio do Peixe	São José de Piranhas	Sapé	Solânea	Soledade	Sousa	Sumé	Uiraúna
Internal Server Error	Baixa	x	x			x		x	x
Autocomplete Enabled	Baixa	x	x	x		x			x
Cookie Not Marked as HttpOnly	Baixa	x	x	x		x			x
Database Error Message Disclosure	Baixa				x				
Programming Error Message	Baixa			x		x			
Out-of-date Version (Apache)	Baixa	x							x
Out-of-date Version (Nginx)	Baixa	x							x
Version Disclosure (PHP)	Baixa			x		x	x	x	
Version Disclosure (Apache)	Baixa	x							x
Version Disclosure (OpenSSL)	Baixa	x							x
Version Disclosure (Apache Module)	Baixa	x							x
Version Disclosure (mod_ssl)	Baixa	x							x
Version Disclosure (Nginx)	Baixa	x							x
Programming Error Message	Baixa						x		
Insecure Frame (External)	Baixa	x		x	x	x	x		x
Missing X-Frame-Options Header	Baixa	x	x	x	x	x	x	x	x
Missing Content-Type Header	Baixa					x			
Insecure Transportation Security Protocol Supported (TLS 1.0)	Baixa	x	x	x	x	x	x	x	x
[Possible] Internal IP Address Disclosure	Baixa			x			x		
[Possible] Cross-site Request Forgery	Baixa		x	x	x	x	x		x
[Possible] Cross-site Request Forgery in Login Form	Baixa		x	x		x			x
[Possible] Phishing by Navigating Browser Tabs	Baixa		x	x	x	x	x		x
Misconfigured Access-Control-Allow-Origin Header	Baixa	x				x		x	x
Mixed Content over HTTPS	Baixa	x				x		x	x

Fonte: Dados da pesquisa (2017).

APENDICE B – Alertas e Informações

		MUNICÍPIOS							
VULNERABILIDADE	CRITICIDADE	Alagoa Grande	Alagoa Nova	Alhandra	Areia	Bananeiras	Belém	Boqueirão	Cabedelo
Forbidden Resource	Alerta	x		x	x	x	x	x	x
Database Detected (MySQL)	Alerta								x
Directory Listing (Apache)	Alerta	x			x	x	x	x	
Email Address Disclosure	Alerta	x		x	x	x	x	x	x
Robots.txt Detected	Alerta	x	x		x		x	x	
Intermediate Certificate is Signed Using a Weak Signature Algorithm	Alerta					x	x		
Generic Email Address Disclosure	Alerta	x			x	x	x	x	
HTTP Strict Transport Security (HSTS) Policy Not Enabled	Alerta	x		x	x	x	x	x	
WordPress Detected	Alerta	x			x	x	x	x	
OPTIONS Method Enabled	Alerta	x	x	x	x	x	x	x	x
Autocomplete Enabled (Password Field)	Alerta	x		x	x	x	x	x	x
Nginx Web Server Identified	Alerta							x	
Apache Web Server Identified	Alerta	x			x	x	x	x	
Out-of-date Version (jQuery)	Alerta					x		x	
Out-of-date Version (jQuery UI Dialog)	Alerta	x			x	x	x	x	
Out-of-date Version (jQuery UI Autocomplete)	Alerta	x			x	x	x	x	
Out-of-date Version (jQuery UI Tooltip)	Alerta	x			x	x	x	x	
Out-of-date Version (jPlayer)	Alerta	x			x	x	x		
Out-of-date Version (Plupload)	Alerta	x			x	x	x	x	
Missing X-XSS Protection Header	Alerta	x	x	x	x	x	x	x	x
SameSite Cookie Not Implemented	Alerta	x		x	x	x	x	x	x
Subresource Integrity (SRI) Not Implemented	Alerta	x		x	x	x	x	x	x
Content Security Policy (CSP) Not Implemented	Alerta	x	x	x	x	x	x	x	x
[Possible] Internal Path Disclosure (*nix)	Alerta	x			x	x	x	x	x

		MUNICÍPIOS							
VULNERABILIDADE	CRITICIDADE	Cajazeiras	Catolé	Conde	Esperança	Guarabira	Itabaiana	Itaporanga	João Pessoa
Forbidden Resource	Alerta	x	x	x	x	x		x	x
Database Detected (MySQL)	Alerta						x		
Directory Listing (Apache)	Alerta	x					x		
Email Address Disclosure	Alerta	x	x	x		x	x	x	x
Robots.txt Detected	Alerta	x		x		x			x
Unexpected Redirect Response Body (Too Large)	Alerta			x					
Intermediate Certificate is Signed Using a Weak Signature Algorithm	Alerta		x	x		x	x	x	x
Generic Email Address Disclosure	Alerta	x	x			x	x		
HTTP Strict Transport Security (HSTS) Policy Not Enabled	Alerta	x	x		x	x	x	x	
WordPress Detected	Alerta	x			x	x			x
OPTIONS Method Enabled	Alerta	x	x	x	x	x	x	x	
Autocomplete Enabled (Password Field)	Alerta	x	x	x				x	
Nginx Web Server Identified	Alerta	x	x		x			x	x
Apache Web Server Identified	Alerta	x	x	x	x	x	x	x	x
Out-of-date Version (jQuery)	Alerta	x	x					x	x
Out-of-date Version (jQuery UI Dialog)	Alerta	x		x					
Out-of-date Version (jQuery UI Autocomplete)	Alerta	x		x					
Out-of-date Version (jQuery UI Tooltip)	Alerta	x							
Out-of-date Version (jPlayer)	Alerta	x							
Out-of-date Version (Plupload)	Alerta	x							
Missing X-XSS Protection Header	Alerta	x	x	x	x	x	x	x	x
SameSite Cookie Not Implemented	Alerta	x	x	x		x		x	x
Subresource Integrity (SRI) Not Implemented	Alerta	x	x		x	x	x	x	x

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		Lagoa Seca	Lucena	Mamanguape	Mari	Mataraca	Patos	Pedras de Fogo	Picuí
Forbidden Resource	Alerta	x	x	x	x		x	x	
Directory Listing (Apache)	Alerta			x	x	x			
Email Address Disclosure	Alerta		x	x	x	x	x	x	
Robots.txt Detected	Alerta			x	x	x	x	x	
Intermediate Certificate is Signed Using a Weak	Alerta		x	x			x	x	x
Generic Email Address Disclosure	Alerta			x	x	x			
HTTP Strict Transport Security (HSTS) Policy Not Enabled	Alerta	x	x	x	x	x	x	x	x
WordPress Detected	Alerta			x	x	x		x	
OPTIONS Method Enabled	Alerta	x	x	x	x	x	x	x	
Autocomplete Enabled (Password Field)	Alerta			x	x	x	x	x	
Nginx Web Server Identified	Alerta						x		
Apache Web Server Identified	Alerta	x	x	x	x	x	x		x
Out-of-date Version (jQuery)	Alerta		x					x	
Out-of-date Version (jQuery UI Dialog)	Alerta		x		x	x			
Out-of-date Version (jQuery UI Autocomplete)	Alerta		x	x	x	x			
Out-of-date Version (jQuery UI Tooltip)	Alerta		x		x	x			
Out-of-date Version (jPlayer)	Alerta				x				
Out-of-date Version (Plupload)	Alerta			x	x	x			
Missing X-XSS Protection Header	Alerta	x	x	x	x	x	x	x	x
SameSite Cookie Not Implemented	Alerta			x	x	x	x	x	
Subresource Integrity (SRI) Not Implemented	Alerta		x	x	x	x	x	x	x
Content Security Policy (CSP) Not Implemented	Alerta	x	x	x	x	x	x	x	x
[Possible] Internal Path Disclosure (*nix)	Alerta		x	x	x	x	x		
[Possible] Administration Page Detected	Alerta						x	x	

VULNERABILIDADE	CRITICIDADE	MUNICÍPIOS							
		Pocinhos	Pombal	Queimadas	Remigio	Rio Tinto	Santa Luzia	Santa Rita	São Bento
Forbidden Resource	Alerta	x	x		x	x	x	x	x
Database Detected (MySQL)	Alerta			x					
Directory Listing (Apache)	Alerta	x				x		x	x
Email Address Disclosure	Alerta	x	x	x		x		x	x
Robots.txt Detected	Alerta		x		x	x	x		x
Intermediate Certificate is Signed Using a Weak	Alerta	x		x		x	x	x	
Generic Email Address Disclosure	Alerta					x		x	
HTTP Strict Transport Security (HSTS) Policy Not Enabled	Alerta	x	x	x	x	x		x	x
WordPress Detected	Alerta				x	x	x	x	x
OPTIONS Method Enabled	Alerta	x	x	x	x	x	x	x	x
Autocomplete Enabled (Password Field)	Alerta		x			x	x	x	x
Nginx Web Server Identified	Alerta		x						
Apache Web Server Identified	Alerta	x	x	x	x	x	x	x	x
Out-of-date Version (jQuery)	Alerta		x		x			x	
Out-of-date Version (jQuery UI Dialog)	Alerta					x	x	x	x
Out-of-date Version (jQuery UI Autocomplete)	Alerta					x	x	x	x
Out-of-date Version (jQuery UI Tooltip)	Alerta					x		x	x
Out-of-date Version (jPlayer)	Alerta					x			x
Out-of-date Version (Plupload)	Alerta					x		x	x
Missing X-XSS Protection Header	Alerta	x	x	x	x	x	x	x	x
SameSite Cookie Not Implemented	Alerta		x	x		x	x	x	x
Subresource Integrity (SRI) Not Implemented	Alerta	x	x	x		x	x	x	x
Content Security Policy (CSP) Not Implemented	Alerta	x	x	x	x	x	x	x	x
[Possible] Internal Path Disclosure (*nix)	Alerta		x	x		x		x	x

		MUNICÍPIOS							
VULNERABILIDADE	CRITICIDADE	São João do Rio do Peixe	São José de Piranhas	Sapé	Solânea	Soledade	Sousa	Sumé	Uiraúna
Forbidden Resource	Alerta	x	x	x	x	x	x	x	
Database Detected (MySQL)	Alerta				x		x		
Directory Listing (Apache)	Alerta	x		x		x	x		x
Email Address Disclosure	Alerta	x	x		x	x	x	x	x
Robots.txt Detected	Alerta	x				x			x
Intermediate Certificate is Signed Using a Weak	Alerta	x			x		x		
Generic Email Address Disclosure	Alerta	x				x		x	x
HTTP Strict Transport Security (HSTS) Policy Not Enabled	Alerta	x		x	x	x	x	x	x
WordPress Detected	Alerta	x				x		x	x
OPTIONS Method Enabled	Alerta	x	x	x	x	x	x	x	x
Autocomplete Enabled (Password Field)	Alerta	x	x	x		x			x
Nginx Web Server Identified	Alerta	x		x			x		x
Apache Web Server Identified	Alerta	x	x	x	x	x	x	x	x
Out-of-date Version (jQuery)	Alerta	x				x			x
Out-of-date Version (jQuery UI Dialog)	Alerta	x				x			x
Out-of-date Version (jQuery UI Autocomplete)	Alerta	x				x			x
Out-of-date Version (jQuery UI Tooltip)	Alerta	x				x			x
Out-of-date Version (jPlayer)	Alerta					x			
Out-of-date Version (Plupload)	Alerta	x				x			x
Missing X-XSS Protection Header	Alerta	x	x	x	x	x	x	x	x
SameSite Cookie Not Implemented	Alerta	x	x	x		x			x
Subresource Integrity (SRI) Not Implemented	Alerta	x		x	x	x	x	x	x
Content Security Policy (CSP) Not Implemented	Alerta	x	x	x	x	x	x	x	x
[Possible] Internal Path Disclosure (*nix)	Alerta			x		x	x		x
[Possible] Administration Page Detected	Alerta		x	x					

Fonte: Dados da pesquisa (2017).