PORTAIS DE GOVERNO ELETRÔNICO DOS MUNICÍPIOS DO ESTADO DA PARAÍBA: ANALISE SOB A ÓPTICA DA SEGURANÇA DA INFORMAÇÃO

Emails:
alnio.sena@gmail.com
wagnerjunqueira.araujo@gmail.com

Alnio Suamy de Sena, Wagner Junqueira de Araújo

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, esse projeto de pesquisa tem como objetivo geral analisar as possíveis vulnerabilidades existentes em portais de governo eletrônico dos municípios do Estado da Paraíba. Serão considerados, como população da pesquisa, os 50 municípios que representem maior participação para a composição do Produto Interno Bruto (PIB) do Estado da Paraíba. Para identificar as possíveis vulnerabilidades nos portais de governo eletrônico, será utilizado o software Nestparker que é um *scanner* de vulnerabilidade. Os dados que comporão a pesquisa serão as possíveis vulnerabilidades encontradas, as quais serão classificadas quanto ao seu grau de criticidade. Os resultados apurados de vulnerabilidades serão analisados e, consequentemente, serão sugeridas medidas para minimizar os riscos identificados com base na revisão de literatura.

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 the public administration as support for internal government processes and delivery of the 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 put

information assets in constant danger by taking advantage of the various vulnerabilities in the virtual environment where e-government is inserted. Thus, this research project has a general objective to analyze the possible vulnerabilities existing in e-government portals of Paraíba state cities. The 50 cities that represent the largest share of the Gross Domestic Product (GDP) of the State of Paraíba will be considered as the research population's sample. To identify potential vulnerabilities in e-government portals, a vulnerability scanner, Nestparker software, will be used. The data gathered will be the possible vulnerabilities found, which will be classified according to their degree of criticality. The verified vulnerability results will be analyzed and, consequently, measures will be suggested to minimize the risks identified based on the literature review.

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

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).

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).

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.

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, 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, este estudo pretende responder a seguinte questão de pesquisa: **Quais as possíveis vulnerabilidades existentes em portais de governo eletrônico dos municípios do Estado da Paraíba?**

Para responder a essa questão propõe-se elencar em uma amostra intencional, um conjunto de portais de governo eletrônico referentes aos municípios do Estado da Paraíba, e, nesses, aplicar uma análise que permita identificar as possíveis 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).

Para que o objetivo geral seja atingido, foram definidos os seguintes objetivos específicos, a saber: i) Identificar os portais de governo eletrônico dos municípios do Estado da Paraíba que serão analisados através de pesquisa feita pela *Internet* para verificar os portais existentes; ii) Aplicar os *scanners* de vulnerabilidades nos portais de governo eletrônico dos municípios identificados do Estado da Paraíba; iii) Elaborar um mapa de vulnerabilidades *versus* riscos através dos dados coletados pelo *scanner* de vulnerabilidade; iv) Descrever as possíveis soluções para a correção das vulnerabilidades identificadas nos portais de governo eletrônico dos municípios do Estado da Paraíba.

Esse trabalho 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 trabalho 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 eles 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 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.

Esse projeto de pesquisa foi dividido em seções, a saber: a Introdução que é tratada na primeira seção, na segunda é trabalhado o referencial teórico, na terceira a metodologia e cronograma e por fim as referências.

2 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.

Quanto aos objetivos, esta pesquisa se classifica como descritiva, pois tem como objetivo descrever as características do governo eletrônico, suas vantagens e desafios e ainda, expor os conceitos de segurança da informação e sua importância para a adequada proteção dos sistemas e informações, além de descrever as vulnerabilidades identificadas e propor soluções.

Quanto aos procedimentos, esta pesquisa pode ser classificada como documental, pois se utilizará de material ou conteúdo publicado nos portais de governo eletrônico. Os portais de governo 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, esta pesquisa caracteriza-se como uma pesquisa quantitativa, pois fará a análise numérica dos dados coletados representando-os por meio de gráficos, tabelas e/ou ilustrações. Os resultados apurados de vulnerabilidades serão analisados e, consequentemente serão sugeridas medidas para minimizar os riscos identificados com base na revisão de literatura.

Inicialmente, considerou-se como população as cinco cidades com maior representatividade no Produto Interno Bruto (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 de toda a 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, serão considerados, 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. Serão identificados os endereços dos portais de cada município que irá constituir a amostra desta pesquisa.

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

O Netsparker é um *scanner* de vulnerabilidades. Um *scanner* de vulnerabilidades é 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 será 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 fará 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*.

O Netsparker 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 serão os dados que comporão 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 6 apresenta-se as 10 vulnerabilidades mais críticas em aplicações *Web* identificadas pela OWASP no relatório trienal de 2013.

Quadro 1: 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

Tais vulnerabilidades, após a varredura, serão classificadas pelo grau de criticidade, ou seja, as vulnerabilidades serão agrupadas em categorias de acordo com o risco que representam para o comprometimento da segurança dos portais governamentais analisados. Os graus de criticidade serão divididos em cinco níveis, sendo eles: i) crítico, ii) alto, iii) médio, iv) baixo e v) alerta, sendo o nível crítico o 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.

REFERÊNCIAS

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.

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

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.

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.

GOVERNMENT ACCOUNTABILITY OFFICE. **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.

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.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. 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/IEC 27000**: Information technology - Security techniques - Information security management systems - Overview and Vocabulary. 3. ed. Switzerland, 2014.

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**, p. 9, 2012.

MANDARINO JÚNIOR, Raphael; CANONGIA, Cláudia. **Segurança cibernética no Brasil:** livro verde. Gabinete de Segurança Institucional (GSI), Brasília, DF, 2010, 63 p.

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.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. **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.

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:** 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-SP.

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

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.

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, RJ, 2013, 490p. Disponível em: <https://esr.rnp.br/livro/seg9#p/20>. Acesso em: 25 de out. 2016.

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