# Mecanismos da governança de tecnologia da informação no auxilio ao compartilhamento de informações governamentais sem a perda de confidencialidade dos dados do cidadão

Rodrigo Hickmann Klein, Eric Charles Henri Dorion

**RESUMO**

Todo o governo deveria ter como objetivos fundamentais proteger o bem público, os direitos individuais e a segurança dos cidadãos. Esses objetivos podem criar tensões intrínsecas e paradoxais, quando a segurança conflita com os direitos individuais, como a confidencialidade dos dados do cidadão. Entretanto, o governo eletrônico precisa possibilitar o equilíbrio entre o bem público e a segurança das informações dos cidadãos. Nesse ponto, os Mecanismos de Governança de Tecnologia da Informação (GTI), que visam operacionalizar relacionamentos, estruturas e processos relacionados à tecnologia da informação, permitem operacionalizar a Gestão da Segurança da Informação, possibilitando orquestrar o equilíbrio entre a transparência e a confidencialidade. A presente pesquisa realiza uma revisão da literatura e explora as relações conflitantes, e ainda pouco exploradas, entre os conceitos transparência, confidencialidade, compartilhamento de dados dos cidadãos e mecanismos de GTI na gestão pública.

**Palavras-chave:** Confidencialidade; Governo Eletrônico; Governança de Tecnologia da Informação.

***ABSTRACT***

*Every government should have as a fundamental objective to protect the public good and individual rights and public safety. These goals can create intrinsic and paradoxical tensions when security conflict with individual rights, such as the confidentiality of citizens' data. However, the e-government must enable the balance between the public good and information security of citizens. At that point, the mechanisms of Information Technology Governance, which aim to operationalize relationships, structures, processes related to information technology, allow operationalize the Information Security Management and enable orchestrate the balance between transparency and confidentiality. This exploratory research conducts an review of the literature and explores the conflicting relations, still not well explored, among the concepts of transparency, confidentiality, citizens' data sharing and mechanisms of IT Governance in public management.*

***Keywords*: *Confidentiality; e-Government; IT Governance.***

## 1 INTRODUÇÃO

No decurso das últimas décadas ocorreu uma mudança no enfoque do governo eletrônico, deixando de ser apenas uma ferramenta que incrementava a conveniência da prestação de serviços do governo, para tornar-se também um facilitador da reforma administrativa e um promotor da participação democrática (YILDIZ, 2007). Entretanto, as ameaças provindas da própria sociedade globalizada, como, por exemplo, grupos radicais, terrorismo e o crime organizado; produziram nos governos o desejo de promover o compartilhamento de informações entre suas agências (KAZA et al., 2011; HALCHIN, 2004; SEIFERT, 2004). Isso repercutiu no incremento de algumas iniciativas, entre elas: a) a fusão e partilha de bases de dados do governo (CAIDI e ROSS, 2005); b) o aumento da segurança dos sistemas de informação do governo contra possíveis ataques (HALCHIN, 2004); c) a expansão da quantidade e abrangência da análise de dados e práticas de mineração de dados

(CAIDI e ROSS, 2005; FEINBERG, 2004; SEIFERT, 2004; SEIFERT e RELYEA, 2004) e d) a redução das ressalvas contra a coleta, integração e partilha entre agências das informações pessoais privadas dos cidadãos (CAIDI e ROSS, 2005; REGAN, 2004; SEIFERT e RELYEA, 2004). Todas essas iniciativas criaram uma tendência alarmante em relação à perda do sigilo e levanta questões sobre a confidencialidade dos dados do cidadão e o legítimo uso das informações (YILDIZ, 2007).

Segundo YILDIZ (2007) a mudança de enfoque do governo eletrônico, produziu uma incompatibilidade entre a percepção de segurança e três dos princípios originais do e-government: a) o acesso rápido e fácil a informações do governo; b) o governo aberto e o direito das pessoas de saber; c) a transparência e a responsividade. Nesse contexto, a Governança de TI pode auxiliar, através de seus mecanismos voltados à Segurança da Informação, visando o equilíbrio entre o bem público e a segurança das informações dos cidadãos (DZAZALI et al., 2009; VALDÉS et al., 2011, KNAPP et al., 2011).

Os Mecanismos de Governança de Tecnologia da Informação (GTI), que visam operacionalizar estruturas, processos e relacionamentos organizacionais relacionados à Tecnologia da Informação, permitem operacionalizar a Gestão da Segurança da Informação (GSI), possibilitando a confidencialidade, a disponibilidade, a irrefutabilidade, a integridade dos dados em organizações privadas (DZAZALI et al., 2009; KNAPP et al., 2011; VALDÉS et al., 2011). Sugerimos que seu escopo de uso seja ampliado para que permita orquestrar o equilíbrio entre a proteção dos dados dos cidadãos e a segurança da sociedade.

Neste contexto, a confidencialidade diz respeito à proteção de informações sensíveis contra divulgação não autorizada e determina que as informações devem ser protegidas de acordo com o grau de sigilo de seu conteúdo (ISO/IEC 27002, 2013). Há informações públicas e privadas, porém nem todas as informações privadas precisam ser mantidas de forma confidencial. No entanto, quando uma informação que deveria ser mantida de forma confidencial, perde este requisito, podem ocorrer perdas econômico-financeiras, perdas de vantagem competitiva, de imagem e até mesmo a continuidade do negócio pode ser comprometida (ISO/IEC 27002, 2013).

Traçando um paralelo com organizações privadas que adotaram a Governança de TI (GTI), a GTI junto ao Governo Eletrônico tende a possibilitar a implementação de processos com metas específicas, indicadores de performances, métricas de resultado, níveis de maturidade com papéis claramente definidos e monitorados por auditorias internas (VALDÉS et al., 2011; HARDY, 2006; KNAPP et al., 2011), resultando no aprimoramento da segurança e no equilíbrio entre a proteção dos dados dos cidadãos e a segurança da sociedade (DZAZALI et al., 2009), possibilitando também a orientação e revisão das estratégias, definição e acompanhamentos dos objetivos e metas de desempenho de gestão, a garantia da integridade dos sistemas da organização e o respeito aos princípios da Governança (KNAPP et al., 2011; HARDY, 2006; LÓPEZ POVEDA, 2011).

Portanto, na GTI existem mecanismos destinados à Segurança da Informação e mecanismos destinados à conformidade legal, que podem operacionalizar as ações do Governo Eletrônico perante às legislações pertinentes, perante à transparência e ao acesso a informação pública, como por exemplo, a lei brasileira 12527/2011 (BRASIL, 2011).

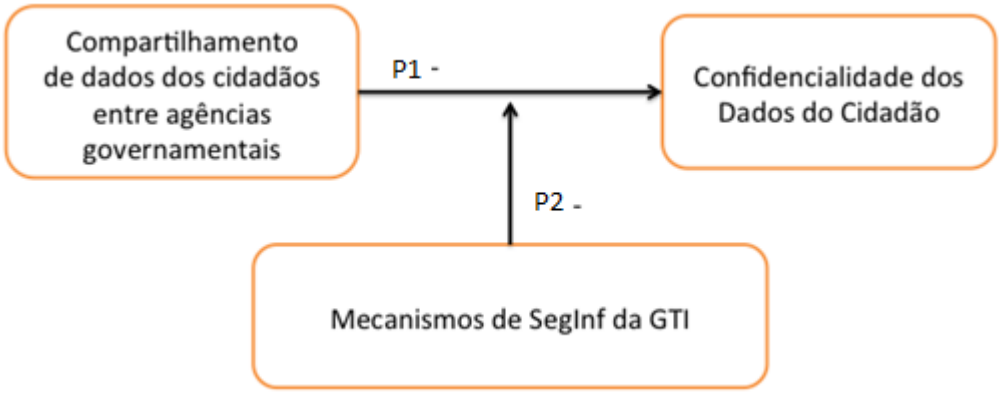
Neste contexto, derivam as seguintes proposições:

**P1**: O compartilhamento de dados dos cidadãos entre agências governamentais influencia negativamente na confidencialidade dos dados do cidadão.

**P2:** A implementação de mecanismos relativos à Segurança da Informação, oriundos da Governança de Tecnologia da Informação, pode auxiliar no compartilhamento de informações governamentais sem a perda da confidencialidade do cidadão.

A Figura 1 demonstra uma representação gráfica destas proposições.

Figura 1 – Representação gráfica das proposições P1 e P2




Neste sentido, diversas pesquisa exploram questões relativas à confidencialidade contemplada pelos mecanismos de SegInf da GTI, e questões da confidencialidade dos dados do cidadão como uma preocupação do e-Government, decorrendo as seguintes proposições:

**P3**: A confidencialidade é uma das preocupações da GTI (IT-Governance) e há mecanismos de SegInf (Segurança da Informação), oriundos da GTI, destinados à confidencialidade, utilizados em organizações privadas.

**P4**: A confidencialidade dos dados do cidadão é uma das preocupações do Governo Eletrônico (e-Government).

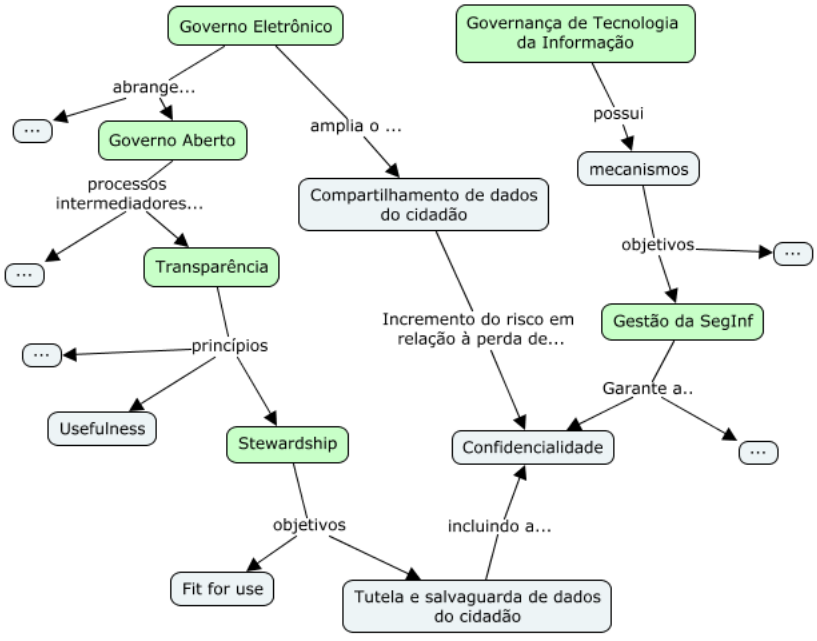
Por outro lado, poucas pesquisas exploram a relação entre os conceitos abordados, decorrendo a seguinte proposição:

**P5**: Há uma área de pesquisa a ser explorada, abordando o uso de mecanismos de Segurança da Informação, oriundos da Governança de Tecnologia da Informação (IT GOVERNANCE), no auxilio à confidencialidade (CONFIDENTIALITY) dos dados do cidadão no Governo Eletrônico (E-GOVERNMENT).

Para ampliar a compreensão a respeito destas proposições, os principais conceitos envolvidos são expostos no referencial teórico.

Os relacionamentos entre estes conceitos, conforme o enfoque desta pesquisa, constam no mapa conceitual, apresentado na Figura 2.

Figura 2 – Mapa conceitual



A seguir será apresentado o referencial teórico com base nos artigos identificados na metodologia, que consta na terceira parte desta pesquisa e ao final são apresentadas as considerações finais.

## 2 REFERENCIAL TEÓRICO

Tento em vista as proposições P1 e P2 e a análise bibliográfica realizada, os principais aspectos sobre os conceitos Governança de Tecnologia da Informação e Segurança da Informação serão destacados a seguir. O referencial teórico enfatiza o relacionamento entre estes conceitos, buscando relacioná-los ao conceito e contexto do Governo Eletrônico.

### 2.1 GOVERNO ELETRÔNICO

Dentre as várias definições sobre governo eletrônico, a definição de Benbasat et al. (2007) sintetiza as definições de vários autores dessa área de estudo, pois define o governo eletrônico como a aplicação da Tecnologia da Informação para permitir trocas interativas de informação entre instituições públicas e suas partes interessadas (*stakeholders*), a fim de fornecer a essas partes interessadas acesso mais fácil à informação governamental e a serviços públicos, quando comparado a outros meios de acesso sem o uso de Tecnologia da Informação.

Entretanto, em relação às categorias de governo eletrônico, a categorização de Belanger e Hiller (2006) é uma da mais abrangente e define as categorias de Governo Eletrônico em dois conjuntos de categorias. O primeiro conjunto agrupa as categorias na qual o fornecimento de informações e serviços ocorre a partir do governo: a) Governo – para – cidadão (G2C); b) Governo – para – empregado (G2E); c) Governo – para – governo (G2G) e d) Governo – para– negócios (G2B). O segundo conjunto engloba categorias nas quais o fornecimento de informações e serviços ocorrem em ambos os sentidos: e) Governo com os indivíduos – Serviços de entrega (GwiS); f) Governo com os indivíduos – processo político (GwiP); g) Governo em negócios com o cidadão (GwBC); h) Governo em negócios com o mercado (GwBMKT); i) Governo com os empregados governamentais (GwE) e j) Governo com governo (GwG).

Considerando a definição de Benbasat et al. (2007), os mecanismos Governança de TI (GTI) destinados a operacionalizar a Segurança da Informação poderão auxiliar em todas as categorias de governo, pois em todas elas há a troca de informação, que devem ser assegurada por processos maduros, auditáveis, controlados por objetivos, com métricas, indicadores, fatores críticos e papéis definidos (KNAPP et al., 2011; HARDY, 2006; LÓPEZ POVEDA, 2011), bem como no Governo Aberto.

### 2.2 GOVERNO ABERTO

De acordo com a Parceria para Governo Aberto (OGP na sigla em inglês), não existe um conceito único de Governo Aberto. No entanto, há princípios que estão presentes em praticamente todas as definições acerca do tema, pois para o governo ser considerado aberto, ele deve buscar alcançar quatro objetivos que são: a) aumentar a disponibilidade de informações sobre atividades governamentais; b) apoiar a participação social; c) implementar os padrões mais altos de integridade profissional na Administração Pública; d) aumentar o acesso a novas tecnologias que promovam a transparência e *accountability*.

De acordo com a Organização para Cooperação e Desenvolvimento Econômico (OECD na sigla em inglês), para a construção de um Governo Aberto existem três princípios-chave a serem levados em consideração: a) *accountability*: existência de mecanismos que possibilitem a identificação e responsabilização dos servidores públicos por suas ações; b) transparência: disponibilização de informações confiáveis, relevantes e tempestivas sobre as atividades do governo; c) participação social: o governo deve escutar os cidadãos e empresas

e levar em consideração os seus anseios tanto no desenho quanto na implementação das políticas públicas (UBALDI, 2013).

Dessa forma, o Governo Aberto disponibiliza dados e compartilha informações que tornam os cidadãos conhecedores da sua realidade social, como por exemplo, através dos Dados Abertos Governamentais (DAGs). Os DAGs permitem que ocorra controle social, fortalecimento da democracia, cidadania ativa, melhorias na administração pública, inovação, cooperação e transparência (HARRISSON et al., 2012). Portanto, devem estar em formato aberto, acessíveis, legíveis por máquina e a informação produzida a partir deles deve ser produzida por todos e para todos (HARRISSON et al., 2012).

No entanto, o Governo Aberto envolve decisões e negociações políticas, bem como ampliação do diálogo com a sociedade para a promoção da transparência e do acesso à informação. Permitindo, por exemplo, criar um diálogo efetivo entre o Estado e a sociedade civil, bem como efetivar a participação dos cidadãos nas discussões sobre a elaboração e a prática das políticas públicas (SCHOLL, 2012).

## 2.3 TRANSPARÊNCIA

De acordo com De Ferranti et al. (2009), a transparência, em termos de governo, refere-se à disponibilidade pública e oportuna, com qualidade, abrangente e relevante, de informações confiáveis sobre as atividades do governo, sendo essencial para fornecer uma base contínua para a aprovação do governante pelo cidadão. Abrangendo a divulgação voluntária e rotineira dos orçamentos, auditorias, políticas e ações executivas, permitindo aos cidadãos avaliarem a eficácia da ação administrativa e fazer exigências sobre os serviços públicos que são prestados pelo governo. Conforme Harrisson et al. (2012) esses atos coincidentemente também geram pressão para melhorar o desempenho, fornecendo ao cidadão um feedback contínuo e permitindo avaliações mais abrangentes dos serviços governamentais.

Segundo Harrisson et al. (2012) as relações entre a informação, a transparência e a democracia são fundamentais e básicas, a informação é essencial para o desenvolvimento de competências democráticas básicas, como por exemplo, a formulação de preferências e opiniões, a conjuntura de hipóteses e a participação na tomada decisão, sem essas competências é negada a voz ao cidadão e o exercício de seus direitos.

No Brasil, a Lei nº 12.527 (BRASIL, 2011), denominada Lei de Acesso a Informação, sancionada em 18 de novembro de 2011, tem o propósito de regulamentar o direito constitucional de acesso dos cidadãos às informações públicas e seus dispositivos são aplicáveis aos três Poderes da União, Estados, Distrito Federal e Municípios. Estabelece que órgãos e entidades públicas devem divulgar informações de interesse coletivo, salvo aquelas cuja confidencialidade esteja prevista no texto legal. Isto deverá ser feito através de todos os meios disponíveis e obrigatoriamente em sites da internet.

A publicação da Lei de Acesso a Informação significa um importante passo para ações de prevenção da corrupção no país, por tornar possível uma maior participação popular, o controle social das ações governamentais e o acesso da sociedade às informações públicas permite que ocorra uma melhoria na gestão pública. No Brasil (BRASIL, 1988), o direito de acesso à informação pública foi previsto na Constituição Federal, no artigo 5º, inciso XXXIII do Capítulo I - dos Direitos e Deveres Individuais e Coletivos - que dispõe que: “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”. A Constituição também tratou do acesso à informação pública no Art. 5º, inciso XIV, Art. 37, § 3º, inciso II e no Art. 216, § 2º.

Entretanto, apesar do incentivo à ampla divulgação dos dados das organizações

governamentais e dos serviços utilizados pelo cidadão, não é do interesse do cidadão que todos seus dados disponibilizados ao governo sejam abertos publicamente, ou distribuídos entre órgãos e esferas governamentais desnecessariamente. Como exemplo, o governo deve divulgar amplamente os dados sobre medicamentos distribuídos à população, porém não deve divulgar qual cidadão consumiu qual remédio. A mesma preocupação com a confidencialidade aplica-se aos dados do imposto de renda fornecido pelo cidadão ao governo. Portanto, o governo precisa gestionar cuidadosa e responsável à informação confiada a ele, neste ponto torna-se crucial um dos princípios da Transparência denominado *Stewardship* (DAWES, 2010).

## 2.4 *STEWARDSHIP*

Toda a informação disponibilizada pelo governo deve atender a requisitos da informação (DAWES, 2010), que podem ser garantidos por mecanismos da Segurança da Informação (ISO/IEC 27002, 2013) constantes em diferentes frameworks de Governança de TI. Consoante a estes requisitos de segurança, Dawes (2010) destaca o *Stewardship* como um dos princípios da Transparência, que está relacionado à gestão cuidadosa e responsável de algo confiado a alguém e quando aplicado à informação concentra-se em garantir a precisão, validade, segurança, gestão e preservação das informações sobre a tutela de alguém. Por este princípio, todos os oficiais públicos e organizações governamentais são responsáveis pela manipulação de informações com cuidado e integridade, independentemente da sua finalidade ou fonte (DAWES, 2010), exigindo que as informações governamentais sejam adquiridas, usadas e gerenciadas como um recurso que tem valor organizacional, jurídico e social, para os diversos propósitos e através do tempo (DAWES, 1996). Portanto, no contexto da transparência, *stewardship* é a proteção das informações do governo contra danos, perda ou uso indevido e torna a informação "*fit for use*" (DAWES, 2010).

Dessa forma, a informação precisa atender alguns requisitos de segurança para manter-se útil e adequada ao uso para o qual foi gerada (ISO/IEC 27002, 2013; DAWES, 2010). Em todas as etapas do ciclo de vida da informação, que são: a coleta ou geração da informação, a utilização, a transformação, o armazenamento, a transmissão e o descarte, a informação deve ser mantida de forma confidencial, precisa se manter íntegra, autêntica e confiável, estar disponível e ser irrefutável, mantendo sempre conformidade a regulatórios. Esses requisitos são especificamente pertinentes à proteção da informação e se complementam aos critérios da informação correta, precisa, completa, relação custo benefício adequada, flexível, relevante, simples, em tempo, verificável e eficaz (PRADO et al., 2014).

Dentre os principais requisitos da informação destacam-se os seguintes:

a) Confidencialidade: diz respeito à proteção de informações sensíveis contra divulgação não autorizada e que as informações devem ser protegidas de acordo com o grau de sigilo de seu conteúdo (ISO/IEC 27002, 2013). Há informações públicas e privadas, porém nem todas as informações privadas precisam ser mantidas de forma confidencial (ISO/IEC 27000, 2014).

b) Integridade: se refere à exatidão e completude das informações, bem como a sua validade, de acordo com os valores de negócios e expectativas no sentido de proteger a exatidão e a completude dos ativos de informação, além dos caminhos pelos quais ela é processada (ISO/IEC 27000, 2014), A integridade da informação pode ser perdida por erros de sistemas ou acesso indevido que venha de dentro ou de fora de uma organização. As consequências da perda de integridade envolvem uma decisão tomada com base em uma informação que perdeu a sua exatidão, que não é mais fidedigna (ISO/IEC 27000, 2014).

c) Disponibilidade: visa garantir que a informação esteja disponível no exato momento em que for necessária. Diz respeito também à salvaguarda dos recursos necessários e capacidades associadas ao acesso a esta informação (ISO/IEC 27002, 2013). Uma informação

não disponível quando necessária pode gerar desde problemas na tomada de decisão até a indisponibilidade de serviços. Por exemplo, um cliente acessa o site da Receita Federal e os dados do seu imposto de renda não estão disponíveis. Esta situação fere a relação de prestação de serviços entre o governo e o cidadão, em virtude da indisponibilidade da informação.

d) Autenticidade: é a propriedade que indica que uma entidade é o que afirma ser (ISO/IEC 27000, 2014). Desta forma, deve-se assegurar que uma informação é autêntica envolve o processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação, ou que são parte de uma determinada transação eletrônica, permitindo o acesso à informação com o devido controle (ISO/IEC 27000, 2014).

e) Confiabilidade: indica à prestação de informação apropriada para as organizações operarem e exercerem suas responsabilidades fiduciárias e de governança (ISO/IEC 27002, 2013). O critério da confiabilidade da informação garante a autoria das informações armazenadas nos Sistemas de Informação.

f) Conformidade: é o atendimento a um requisito (ISO/IEC 27000, 2014), o que significa, em um contexto de Segurança da Informação, que a informação deve ser mantida em conformidade com o regulatório a qual está sujeita em todo o ciclo de vida, ou seja, desde a sua geração até o seu descarte. A conformidade envolve aderência a leis, regulamentos e acordos contratuais e políticas externas às quais um determinado processo de negócio está sujeito. Entre os regulatórios, com os quais organizações poderiam necessitar estar em conformidade, podemos citar a Lei nº 12.527 (BRASIL, 2011) de acesso à informação. A conformidade, uma vez estabelecida, deve ser mantida em todo o ciclo de vida da informação, mostrando garantias de que a informação não é resultante de uma alteração indevida.

g) Irrefutabilidade: ocorre quando o remetente ou autor de uma informação não pode negar que a enviou ou que a gerou, constituindo uma forma estrita de autenticação e pode ser obtida mediante uma assinatura eletrônica (ISO/IEC 27000, 2014). Desta forma, se constitui em um requisito prévio indispensável para a realização de muitas ações e serviços, como compras eletrônicas através da internet. Conhecida também como não-repúdio, garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita (ISO/IEC 27000, 2014). Como, por exemplo, um documento liberado por algum órgão de governo deve ter sua autoria, sua responsabilidade técnica, autenticada de forma que não possa ser refutada.

Os principais requisitos de informações oriundas da transparência podem ser garantidos pela Gestão da Segurança da Informação (GSI), que por usa vez, pode ser incluída dentre os mecanismos da Governança de Tecnologia da Informação (SOLMS, 2005; ITGI, 2007).

## 2.5 GESTÃO DA SEGURANÇA DA INFORMAÇÃO (GSI)

A GSI é o processo responsável por garantir que a confidencialidade, integridade e disponibilidade dos ativos, informações, dados e serviços de TI de uma organização correspondam às necessidades acordadas do negócio (ISO/IEC 27002, 2013). A ISO 27002 (ISO/IEC 27002, 2013) define segurança da informação como a proteção da informação contra diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando os danos aos negócios, maximizando o retorno dos investimentos e as oportunidades de negócio. Segundo essa norma, a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados quando e onde for necessário, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos.

Na ISO 27002 (ISO/IEC 27002, 2013) é enfatizado que um SGSI (Sistema de Gestão de Segurança da Informação) deve ser implementado de acordo com as necessidades e porte

da organização. O escopo e os limites do SGSI precisam estar balizados pelos termos e características do negócio, da organização, da localização e dos ativos de tecnologia. O SGSI necessita incluir uma estrutura para definir objetivos e estabelecer um direcionamento global, além de abranger os princípios para as ações relacionadas à segurança da informação, considerando os requisitos de negócio, legais ou regulamentares. Contemplando também as obrigações de segurança contratuais e alinhamento com o contexto estratégico de gestão de risco da organização, estabelecendo critérios em relação aos riscos que serão avaliados e por fim, definindo a abordagem de análise e avaliação de riscos da organização (ISO/IEC 27002, 2013).

## 2.6 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

Segundo Sambamurthy e Zmud (1999) Governança de Tecnologia da Informação (GTI) é a especificação de estruturas de tomada de decisão, processos e mecanismos relacionais para direção e controle de operações de Tecnologia da Informação. Segundo Weill e Ross (2004) a GTI pode ser entendida como a especificação de direitos decisórios e de um framework de responsabilidades para estimular os comportamentos desejados na utilização de Tecnologia da Informação (TI).

Para Van Grembergem, De Haes e Guldentops (2004) a GTI caracteriza-se por um conjunto de arranjos e práticas associadas à estrutura, processos e relacionamentos. Esse conjunto de arranjos e práticas, também chamado de mecanismos e viabilizam a aplicação prática dos princípios e definições da GTI de uma organização, tornando tangíveis as definições de alto nível acerca de como a TI de uma organização deve operar. Dessa forma, os mecanismos de GTI podem ser compreendidos como procedimentos, artefatos ou um conjunto de ações, que devem estar sempre associados a um ou mais objetivos da Governança de TI (VAN GREMBERGEM, DE HAES e GULDENTOPS, 2004).

Conforme De Haes e Van Grembergen (2005) a Governança de TI pode ser implantada usando uma combinação de estruturas, processos e mecanismos relacionais, onde: a) estruturas correspondem a papéis e responsabilidades, estrutura e organização da TI, CIO no conselho administrativo, Comitê de Estratégia de TI, Comitê Gestor de TI; b) processos correspondem a Planejamento Estratégico de Sistemas de Informação, BSC (*Balanced Score Card*) de TI, Informações Econômicas, Acordos de Nível de Serviço, COBIT e ITIL, Modelos de alinhamento de TI e níveis de maturidade de governança; e c) mecanismos de relacionamento correspondem à participação ativa e a colaboração entre as principais partes interessadas, parceria de recompensas e incentivos, *co-location* entre negócio e TI, formação e rotação *cross-funcional* entre TI e negócio. Portanto, segundo os autores, as estruturas envolvem a existência de funções em nível de gerência e chefia, como executivos de TI, além de uma diversidade de comitês de TI. Sendo que os processos referem-se à tomada de decisões estratégicas e monitoramento via, como por exemplo, o BSC de TI, e os mecanismos de relacionamento incluem a participação da TI no negócio, o diálogo estratégico, a aprendizagem compartilhada e a comunicação adequada. Cada uma destas práticas serve a objetivos múltiplos ou específicos na GTI (DE HAES e VAN GREMBERGEN, 2005).

No entanto, de acordo com De Haes e Van Grembergen (2005), a divisão da complexidade da GTI em pedaços menores e a resolução de cada problema separadamente nem sempre resolve o problema completo, pois é necessária uma abordagem holística, reconhecendo a natureza complexa e dinâmica da GTI, que é consistida de um conjunto de subsistemas interdependentes que proporcionam um conjunto necessário para um bem sucedido *framework* de implementação de GTI. Portanto, consiste em uma combinação de estruturas, processos e mecanismos relacionais que dependem das múltiplas contingências, com uma combinação ideal, que pode variar em cada organização (DE HAES e VAN GREMBERGEN, 2005).

Contudo, as organizações privadas que investem na implementação da GTI, em busca da conformidade com normas regulatórias, como por exemplo, a SOX (SPEARS et al., 2010), acabam por obter uma série de outros benefícios, tal como, a efetividade dos processos e controles (DE HAESE e VAN GREMBERGEN, 2009) e alguns desses controles operacionalizam a Gestão da Segurança da Informação (GSI) (SOLMS, 2005; ITGI, 2007), pois a GTI consiste na liderança, estruturas organizacionais e processos que garantam que a organização da TI sustente e estenda a estratégia da organização e seus objetivos (DE HAES e VAN GREMBERGEN, 2008). Por outro lado, algumas organizações que não necessitam dessas regulamentações desconhecem demais benefícios da Governança de TI, como os benefícios que podem ser obtidos na área da Segurança da Informação.

Assim como a conformidade legal com leis de acesso informação, a GTI possibilita a implementação de processos com metas específicas, indicadores de performances, métricas de resultado, níveis de maturidade papéis claramente definidos e monitorados por auditorias internas (VALDÉS et al., 2011; HARDY, 2006; KNAPP et al., 2011), resultando no aprimoramento da segurança e no equilíbrio entre a proteção dos dados dos cidadãos e a segurança da sociedade (DZAZALI et al., 2009), possibilitando também a orientação e revisão das estratégias, definição e acompanhamentos dos objetivos e metas de desempenho de gestão, a garantia da integridade dos sistemas da organização e o respeito aos princípios da Governança (KNAPP et al., 2011; HARDY, 2006; LÓPEZ POVEDA, 2011). Além de, financeiramente, proporcionar melhoras significativas em seu desempenho organizacional, especialmente em relação às medidas de rentabilidade, quando comparadas às empresas do mesmo setor sem tais mecanismos implementado, permitindo afirmar que a adoção de práticas de governança de TI está associada à melhoria de diferentes métricas financeiras (LUNARDI, BECKER e MAÇADA, 2012) podem trazer também benefícios financeiros governamentais (LÓPEZ POVEDA, 2011).

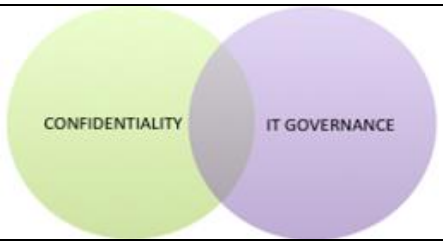
## 3 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa é qualitativa e exploratória. A análise dos dados coletados, oriundos dos artigos publicados sobre o tema, foi realizada por meio de análise de conteúdo indicada por Flick (2009) e apresenta reflexões e proposições com base em uma revisão sistemática desta literatura, com o objetivo de analisar de forma crítica e gerar uma síntese dos resultados de vários estudos. Dessa forma, as proposições apresentadas a seguir são construídas com base nas teorias e conceitos dos artigos encontrados nos Quadros 1, 2 e 3. Os principais artigos, que relacionaram os conceitos pesquisados, foram expostos no referencial teórico.

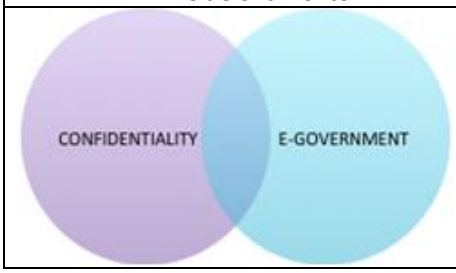
A pesquisa e a análise dos artigos foram realizadas entre 31/05/2015 e 22/07/2015. Foram priorizados os termos que obtiveram resultados exclusivamente relacionados ao conceito, por exemplo, o termo "IT GOVERNANCE" está relacionado ao conceito Governança de Tecnologia da Informação, por outro lado, "INFORMATION TECNOLOGY GOVERNANCE", e demais variações, retornaram um maior número de artigos, porém não estavam relacionados a este conceito.

Em relação ao escopo de pesquisa, utilizou-se o escopo de pesquisa *FULL TEXT*, ou "Texto Completo", procurando o termo em todo artigo. Adicionalmente, no indexador http://search.proquest.com, foram utilizadas as opções "Revisado por especialistas" e "Periódicos acadêmicos". Os termos em inglês limitaram a pesquisa a artigos neste idioma, ou aos artigos que utilizaram palavras chave neste idioma.

Quadro 1- Confidencialidade e Governança de Tecnologia da Informação no mesmo artigo

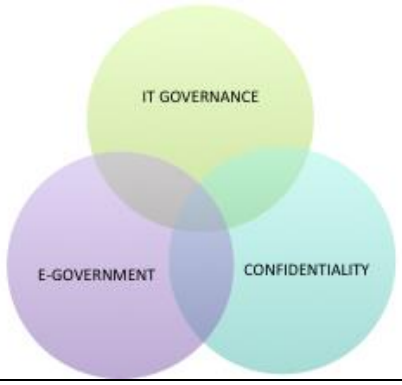
| Termos pesquisados | |
|---|---|
| **"CONFIDENTIALITY" AND "IT GOVERNANCE"** | |
| **Indexadores consultados** | **Total de artigos únicos encontrados em cada indexador** |
| http://www.sciencedirect.com | 71 |
| http://apps.webofknowledge.com | 6 |
| https://doaj.org | 2 |
| http://search.proquest.com | 111 |
| http://www.scopus.com | 7 |
| **Relacionamento** | **Proposição** |
|  | Devido ao constante relacionamento entre os dois termos nos artigos analisados e conforme apresentados no referencial teórico, pode ser confirmada a seguinte proposição:<br>P3: A confidencialidade é uma das preocupações da GTI (IT-Governance) e há mecanismos de SegInf (Segurança da Informação), oriundos da GTI, destinados à confidencialidade, utilizados em organizações privadas. |

Quadro 2 - Confidencialidade e Governo Eletrônico no mesmo artigo

| Termos pesquisados | |
|---|---|
| **"CONFIDENTIALITY" AND "E-GOV"** | |
| **"CONFIDENTIALITY" AND "ELECTRONIC GOVERNMENT"** | |
| **Indexadores consultados** | **Total de artigos únicos encontrados em cada indexador** |
| http://www.sciencedirect.com | 305 |
| http://apps.webofknowledge.com | 41 |
| https://doaj.org/ | 1 |
| http://search.proquest.com/ | 254 |
| http://www.scopus.com | 56 |
| **Relacionamento** | **Proposição** |
|  | Devido ao grande relacionamento entre os dois termos, encontrados nos artigos analisados e apresentado no referencial teórico, pode ser confirmada a seguinte proposição:<br><br>P4: A confidencialidade dos dados do cidadão é um das preocupações da área de pesquisa do Governo Eletrônico (e-Government). |

Quadro 3 - Governança de Tecnologia da Informação, Governo Eletrônico e Confidencialidade no mesmo artigo

| Termos pesquisados | |
|---|---|
| **"CONFIDENTIALITY" AND "IT GOVERNANCE" AND "E-GOV"** | |
| **"CONFIDENTIALITY" AND "IT GOVERNANCE" AND "E-GOVERNMENT"** | |
| **"CONFIDENTIALITY" AND "IT GOVERNANCE" AND "ELECTRONIC GOVERNMENT"** | |
| **Indexadores consultados** | **Total de artigos únicos encontrados em cada indexador** |
| http://www.sciencedirect.com | 6* |
| http://apps.webofknowledge.com | 0 |
| https://doaj.org/ | 0 |
| http://search.proquest.com/ | 12* |
| http://www.scopus.com | 1* |
| *Nos indexadores que obtiveram algum resultado, os termos foram localizados no rodapé, nos títulos de referências e o termo "CONFIDENCIALITY" se aplicava a coleta de dados nas pesquisas. Portanto o resultado equivale a 0 (zero) artigos encontrados. | |

| Relacionamento | Proposição |
|---|---|
|  | Considerando que nenhum artigo relacionamento os três termos nos artigos analisados pode ser confirmada a seguinte proposição:<br><br>P5: Há uma área de pesquisa a ser explorada, abordando o uso de mecanismos de Segurança da Informação, oriundos da Governança de Tecnologia da Informação (IT GOVERNANCE), no auxilio à confidencialidade (CONFIDENTIALITY) dos dados do cidadão no Governo Eletrônico (E-GOVERNMENT). |

## 4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Através do procedimento metodológico aplicado foram encontradas pesquisas mencionando que o compartilhamento de dados dos cidadãos entre agências governamentais influencia negativamente na confidencialidade dos dados do cidadão, pois coloca em risco os dados compartilhados (MCMILLEN, 2004; HALCHIN, 2004; YILDIZ, 2007,; KIERKEGAARD, 2008; BELDAD, et al. 2010), de acordo com a preposição P1.

Por outro lado, a implementação de mecanismos relativos à Segurança da Informação, oriundos da Governança de Tecnologia da Informação, pode auxiliar no compartilhamento de informações sem a perda da confidencialidade (DZAZALI et al., 2009; VALDÉS et al., 2011, KNAPP et al., 2011), conforme indicado pela proposição P2.

A confidencialidade é uma das preocupações da GTI (IT-Governance) e há mecanismos de SegInf (Segurança da Informação) oriundos da GTI, destinados à confidencialidade (TUTTLE e VANDERVELDE, 2007; KNAPP et al., 2011; DZAZALI et al., 2009; VALDÉS et al., 2011), consoante à proposição P3.

A confidencialidade dos dados do cidadão é um das preocupações da área de pesquisa do Governo Eletrônico (e-Government) (MCMILLEN, 2004; HALCHIN, 2004; YILDIZ, 2007; KIERKEGAARD, 2008; BELDAD, et al. 2010), de acordo com a preposição P4.

Entretanto, foi constatada a inexistência de pesquisas que exploram a relação entre os três conceitos Confidencialidade (CONFIDENTIALITY), Governança de Tecnologia da Informação ("IT GOVERNANCE") e Governo Eletrônico (E-GOVERNMENT), nos indexadores pesquisados, conforme proposto pela proposição P5.

Dessa forma, há uma área de pesquisa a ser explorada, abordando o uso de mecanismos de Segurança da Informação, oriundos da Governança de Tecnologia da Informação (IT GOVERNANCE), no auxilio à confidencialidade (CONFIDENTIALITY) dos dados do cidadão no Governo Eletrônico (E-GOVERNMENT). Propomos estudos que envolvendo a aplicabilidade dos mecanismos de Segurança da Informação da GTI no Governo Eletrônico para aprimorar a confidencialidade dos dados do cidadão.

A Governança de Tecnologia da Informação (GTI) não é destinada exclusivamente à Segurança da Informação, porém aborda muitas questões relativas a ela (SOLMS, 2005). A vantagem de usar os controles proporcionados pelos mecanismos de Gestão da Segurança da Informação está na integração dos objetivos de controle de mecanismos da Segurança da Informação, em um âmbito mais amplo, fornecendo uma plataforma integrada entre a arquitetura e a estrutura da Tecnologia da Informação e demais mecanismos (SOLMS, 2005).

Por outro lado, a desvantagem de usar os mecanismos da Gestão da Segurança Informação (GSI) oriundos da GTI é que, na maioria dos casos, não há orientação mais detalhada de "como" as atividades e processo devem ser realizados (SOLMS, 2005). Nesse ponto é viável combinar, por exemplo, a norma ISO/IEC 27002 (ISO/IEC 27002, 2013), pois

a abordagem à Gestão da Segurança da Informação é mais detalhada e fornece orientação mais precisas de como implementar essa gestão (SAHIBUDIN et al., 2008).

## 5 CONSIDERAÇÕES FINAIS

Para que as organizações públicas possam obter os benefícios de orientações mais detalhadas fornecidas pelas práticas de Sistemas de Gestão da Segurança da Informação (SGSI), integrada à GTI, pode ser vantajoso usar os dois conjuntamente na Gestão da Segurança da Informação (GSI) do Governo Eletrônico (e-GOV). A sinergia para combinar essas duas opções pode ser substancial, pois em certa medida, estas duas estruturas naturalmente se complementam (SAHIBUDIN et al., 2008). Sendo possível utilizar a GTI como um elemento de mais alto nível de referência à Gestão da Segurança da Informação, onde "o que" estará bastante claro, e o SGSI (ISO/IEC 27002, 2013) como um nível "inferior", mais detalhado, com orientações específicas para a Segurança da Informação, onde o "como" é ressaltado (SOLMS, 2005).

A Gestão da Segurança da Informação pode ser vista como mais uma dimensão da GTI (SOLMS, 2005), possibilitando implementar o SGSI mais amplo e integrado a GTI (SOLMS, 2005) em organizações públicas que promovem o Governo Aberto, pois os mecanismos de Governança de TI podem propiciar uma maior efetividade e transparência dos investimentos em segurança para os altos escalões das organizações (SPEARS et al., 2010).

Todavia, conforme o conteúdo dos artigos analisados, a confidencialidade é uma das preocupações da GTI e há mecanismos de Segurança da Informação oriundos da GTI destinados à confidencialidade, que já são utilizados em diversas organizações. No mesmo sentido, a confidencialidade dos dados do cidadão é uma das preocupações do Governo Eletrônico. Entretanto, o uso de mecanismos de Segurança da Informação da GTI no auxilio a confidencialidade no Governo Eletrônico não está sendo amplamente explorado pelas pesquisas nesta área.

A GTI pode produzir uma série de benefícios ao governo eletrônico, ao operacionalizar estruturas, processos e relacionamentos organizacionais relacionados à TI, em especial ao foco em questão, possibilitando a confidencialidade, disponibilidade, irrefutabilidade, integridade dos dados dos cidadãos e dos dados disponibilizados pelo governo aberto, orquestrando o equilíbrio entre a proteção dos dados dos cidadãos e a segurança da sociedade.

Todavia, propomos que há uma área de estudo a ser explorada, envolvendo a aplicabilidade dos mecanismos da Gestão da Segurança da Informação da GTI no Governo Eletrônico, e principalmente, na gestão confidencialidade dos dados do cidadão. Estudos que analisem aplicabilidade e as formas de transpor o conhecimento já obtido em instituições privadas, para um contexto governamental.

Entretanto, há limitações na presente pesquisa, pois podem existir artigos científicos que já abranjam o tema proposto, porém com outra terminologia, ou artigos em demais indexadores não pesquisados. Além disso, não há garantia da aplicabilidade do conhecimento e conceitos, já utilizados em organizações privadas, em um novo contexto de organizações públicas.

Contudo, sugerimos pesquisas que visem identificar quais aspectos da GTI favorecem a Gestão da Segurança da Informação dentro do Governo Eletrônico, que permitam indicar as situações nas quais estes aspectos já estão implementadas no Governo Aberto e na disponibilização de Dados Abertos, indicando também as medidas que definem a estrutura formal da Segurança da Informação e se elas possibilitam o atendimento das múltiplas contingências do Governo Eletrônico.

## REFERÊNCIAS

BENBASAT, I.; CENFETELLI, R.; TAN, C. Understanding the antecedents and consequences of e-government service quality: An empirical investigation. **ICIS 2007 Proceedings.** 2007.

BELANGER, F.; HILLER, J. S. A framework for e-government: privacy implications. **Business process management journal**, v. 12, n. 1, p. 48-60, 2006.

BELDAD, A.; DE JONG, M; STEEHOUDER, M. Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. **Government Information Quarterly**, v. 27, n. 3, p. 238-244, 2010.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

CAIDI, N.; ROSS, A. Information rights and national security. **Government Information Quarterly**, v. 22, n. 4, p. 663-684, 2005.

DAWES, S. S. Interagency information sharing: Expected benefits, manageable risks. **Journal of Policy Analysis and Management**, v. 15, n. 3, p. 377-394, 1996.

DAWES, S. S. Stewardship and usefulness: Policy principles for information-based transparency. **Government Information Quarterly**, v. 27, n. 4, p. 377-383, 2010.

DE FERRANTI, D.M.; JACINTO, J.; ODY, A. J.; RAMSHAW, G., How to Improve Governance: a New Framework for Analysis and Action, Brookings Institution Press, 2009. Disponível em: http://books.google.com.br/books?id=2A7F-p17FYEC&lpg=PA8&vq=transparency&dq=How%20to%20Improve%20Governance&hl=pt-BR&pg=PA6#v=snippet&q=timely&f=false. Acesso em: 15 de novembro de 2013.

DE HAES, S.; VAN GREMBERGEN, W. **IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial GroupSystem Sciences**. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on, 2005.

_____. Practices in IT Governance and Business/IT Alignment. **ISACA Journal.** n. 2, ISACA, USA, 2008.

_____. An Exploratory Study Into IT Governance Implementations and its Impact on Business/IT Alignment, **Information Systems Management**, n. 26, v. 2, p. 123-137, Taylor & Francis, UK, 2009.

DOAJ. Disponível em: https://doaj.org. Acesso em 31 mai. 2015.

DZAZALI, S.; SULAIMAN, A.; ZOLAIT, A. H. Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. **Government**

**Information Quarterly**, v. 26, n. 4, p. 584-593, 2009.

FEINBERG, L. E. FOIA, federal information policy, and information availability in a post-9/11 world. **Government Information Quarterly**, v. 21, n. 4, p. 439-460, 2004.

FLICK, U. Introdução à pesquisa qualitativa. 3. ed. Porto Alegre: Artmed, 2009.

HALCHIN, L. E. Electronic government: Government capability and terrorist resource. **Government Information Quarterly**, v. 21, n. 4, p. 406-419, 2004.

HARDY, G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. **Information Security Technical Report**, p. 55–61, 2006.

HARRISSON, T. M. et al. Open government and e-government: Democratic challenges from a public value perspective, **Information Polity**, v. 17, p. 83-97, 2012.

ISO/IEC 27000. International Organization for Standardization and International Electrotechnical Commission. Information technology – security techniques – information security management systems – overview and vocabulary. Genebra: ISO/IEC, 2014.

ISO/IEC 27002. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2013.

ITGI. **Cobit Security Base Line: An Information Security Survival Kit**. IT Governance Institute. 2 ed., 2007.

KAZA, S.; HU, P. J. H.; HU, H. F.; CHEN, H. Designing, implementing, and evaluating information systems for law enforcement—A long-term design-science research project. **Communications of the Association for Information Systems**, v. 29, n. 1, p. 28, 2011.

KIERKEGAARD, S. The Prüm decision–An uncontrolled fishing expedition in 'Big Brother'Europe. **Computer Law & Security Review**, v. 24, n. 3, p. 243-252, 2008.

KNAPP, K. J.; DENNEY, G. D.; BARNER, M. E. Key issues in data center security: An investigation of government audit reports. **Government Information Quarterly**, v. 28, n. 4, p. 533-541, 2011.

LÓPEZ POVEDA, A. **Towards a framework for analyzing IT strategy management in public sector: a case for IT organisations in the public sector**. Tese de Doutorado, KTH, 2011.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. An empirical study of the impact of IT governance on financial performance. **Production**, v. 22, n. 3, p. 612-624, 2012.

MCMILLEN, D. Privacy, confidentiality, and data sharing: Issues and distinctions. **Government Information Quarterly**, v. 21, n. 3, p. 359-382, 2004.

PRADO, E.; ORNELLAS, R.; ARAÚJO, L. Fundamentos de Sistemas de Informação. Elsevier Brasil, 2014.

PROQUEST. Disponível em: http://search.proquest.com. Acesso em 30 mai. 2015.

REGAN, P. M. Old issues, new contexts: Privacy, information collection and homeland security. **Government Information Quarterly**, 21, 481−497, 2004.

SAMBAMURTHY, V.; ZMUD, R. W. Arrangements for information technology governance: A theory of multiple contingencies. **MIS Quarterly**, v. 23, n. 2, p. 261-290, 1999

SAHIBUDIN, S.; SHARIFI, M.; AYAT, M. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. **2008 Second Asia International Conference on Modelling & Simulation (AMS)**, p. 749–753, Ieee, 2008.

SCHOLL, H. J. Five trends that matter: Challenges to 21st century electronic government. **Information Polity**, v. 17, p. 317–327, 2012.

SCIENCE DIRECT. Disponível em: http://www.sciencedirect.com. Acesso em 31 mai. 2015.

SCOPUS. Disponível em: http://www.scopus.com. Acesso em 31 mai. 2015.

SEIFERT, J. W.; RELYEA, H. C. Do you know where your information is in the homeland security era? **Government Information Quarterly**, v. 21, n. 4, p. 399-405, 2004.

SEIFERT, J. W. Data mining and the search for security: Challenges for connecting the dots and databases. **Government Information Quarterly**, v. 21, n. 4, p. 461-480, 2004.

SOLMS, Basie von. Information Security governance: COBIT or ISO 17799 or both? Elsevier Science Ltd. **Computers & Security**. v. 24, n. 2, mar., p. 99-104, 2005.

SPEARS, J. L.; BARKI, H. User Participation in Information Systems Security Risk Management. **MIS Quarterly**, v. 34, n. 3, p. 503-522, 2010.

TUTTLE, B.; VANDERVELDE, S. D. An empirical examination of CobiT as an internal control framework for information technology. International Journal of Accounting Information Systems, v. 8, n. 4, p. 240-263, 2007.

UBALDI, B. Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. OECD Working Papers on Public Governance, No. 22, OECD Publishing, 2013.

VALDÉS, G.; SOLAR, M.; ASTUDILLO, H.; IRIBARREN, M.; CONCHA, G.; VISCONTI, M. Conception, development and implementation of an e-Government maturity model in public agencies. **Government Information Quarterly**, v. 28, n. 2, p. 176-187, 2011.

VAN GREMBERGEN, W., DE HAES, S., GULDENTOPS, E. Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. Information **Systems Control Journal**, v. 6, p. 32-35, 2004.

WEB OF KNOWLEDGE. Disponível em: http://apps.webofknowledge.com. Acesso em 31 mai. 2015.

WEILL P, ROSS JW. IT governance: how top performers manage IT decision rights for superior results. Boston, MA: **Harvard Business School Press**; 2004.

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