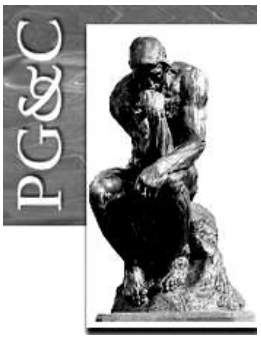


MODELO DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL

Rogério Guimarães
Mestre em Gestão do Conhecimento e da Tecnologia da Informação pela Universidade Católica de Brasília, Brasil.
E-mail: guimaraesrog@gmail.com

João Souza Neto
Doutor em Engenharia Elétrica pela Universidade de Brasília, Brasil.
Professor da Universidade Católica de Brasília, Brasil.
E-mail: joaon@p.ucb.br

Mauricio Rocha Lyra
Doutor em Ciência da Informação pela Universidade de Brasília, Brasil.
Professor do Centro Universitário de Brasília, Brasil.
E-mail: mauricio.lyra@gmail.com

Resumo
A Governança de Segurança da Informação e Comunicações consiste em um conjunto de políticas e processos que permite que as instituições monitorem, avaliem e direcionem a gestão de seus ativos de informação, reduzindo os riscos à sua integridade, confidencialidade e disponibilidade, de forma alinhada com as necessidades de negócios. Esta pesquisa apresenta uma proposta de modelo de Governança de Segurança da Informação e Comunicação para a Administração Pública Federal aderente às normas brasileiras e compatível com a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018. O modelo proposto foi concebido a partir da análise de conteúdo, à luz de critérios específicos, do modelo do NIST 800-100, e da norma ABNT 27014:2013, sendo esta última tomada como padrão estrutural referencial. O modelo proposto foi, em seguida, submetido à avaliação de um grupo focal composto de especialistas em segurança da informação da Administração Pública Federal, sendo considerado adequado à realidade atual da APF por considerar as restrições e requerimentos legais e normativos existentes e as características inerentes ao setor público brasileiro.

Palavras-chave: Governança de Segurança da Informação. *Framework* de Governança de Segurança da Informação.

INFORMATION SECURITY GOVERNANCE MODEL FOR THE BRAZILIAN FEDERAL PUBLIC ADMINISTRATION

Abstract
Information and Communications Security Governance consists of a set of policies and processes which allows institutions to monitor, evaluate and direct its information assets management, reducing risks related to its integrity, confidentiality and availability, aligned with business needs. This research proposes a framework of information and communications security governance for the Federal Government, adhering to Brazilian legal standards and compliant with the Information and Communications Security and Cybersecurity Strategy of the Federal Government 2015 – 2018. The proposed framework was designed using the content analysis methodology, in view of specific criteria of the NIST model 800-100, and of the standard ABNT 2014:2013, the latter was taken as the structural

reference standard. The proposed model was then submitted to evaluation of a focus group composed of information security experts of the Government, considering the existing legal and regulatory restrictions and requirements and the inherent characteristics of the Brazilian public sector.

Keywords: *Information security governance. Information security governance framework.*

1 INTRODUÇÃO

A área de segurança da informação tem evoluído rapidamente, como pode ser observado pela crescente disponibilização de normas, padrões e o uso de boas práticas no ambiente corporativo. O entendimento que segurança da informação é condição para o sucesso e a perenidade dos negócios corporativos torna o tema responsabilidade da alta gestão das organizações. Integrando-se aos demais subconjuntos que compõem a Governança Corporativa, tais como Governança Financeira, Governança de Relacionamentos, Governança de Ativos, Governança de Gestão de Pessoas, entre outros, insere-se a Governança de Segurança da Informação (GovSI).

Na Administração Pública Federal (APF), a análise dos dados levantados pelo Tribunal de Contas da União (TCU) por meio da pesquisa de Perfil de Governança de Tecnologia da Informação – ciclo 2014, no que se refere à evolução das práticas relativas às políticas e responsabilidades de segurança da informação, conclui que, a despeito da evolução identificada no período 2012 a 2014, o nível de adoção das práticas apresentadas está muito aquém do esperado, situação que 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.

Ainda em relação à administração pública, a pesquisa sobre maturidade de governança de segurança da informação na APF, conduzida por Britto (2011, p. 72), conclui que "[...] Os motivos apresentados pelos ministérios refletem uma falta de interesse da alta administração em alinhar a Segurança de Informação com a estratégia e serviços providos pelos órgãos".

Em maio de 2015, o Conselho de Defesa Nacional publicou a Portaria n° 14 (CDN, 2015), em atenção à recomendação do Acórdão 3.051/2014-TCU-Plenário. Nesta apresenta a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0, elaborada pelo Departamento de Segurança da Informação e Comunicações (DSIC), órgão subordinado ao Gabinete de Segurança Institucional da Presidência da República). A Estratégia (2015, p. 65) considera que:

> [...] dado que tais áreas são consideradas como questões nacionais, horizontais e estratégicas, que afetam todos os níveis da sociedade, e representa importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, objetivando melhorar sobremaneira a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais [...]

Destaca-se, ainda, no texto introdutório do documento do DSIC que, apesar do arcabouço normativo publicado nos últimos oito anos pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) sobre Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética, o nível de maturidade dos órgãos e entidades da APF ainda encontra-se em patamar aquém do desejado.

A Estratégia explicita, em seu Objetivo Estratégico OE-IV, a necessidade de instituir um modelo de governança sistêmica de SIC e Segurança Cibernética (Segciber) na APF, bem como conclama a participação da Academia para execução da Estratégia.

Diante do contexto, é premente a necessidade de adoção de um modelo de GovSI que promova ações coordenadas, orientando e direcionando os órgãos e instituições da APF no sentido de adotar ações efetivas e, consequentemente, melhorarem os níveis individuais de Governança de Segurança da Informação e Comunicação, uma vez que os achados obtidos no levantamento do TCU sugerem que há um profundo desalinhamento entre as ações de segurança da informação e os requisitos de segurança da informação estabelecidos pelas políticas públicas, o que causa perda de eficiência e aumento de custos na gestão dos riscos.

2 REVISÃO DE LITERATURA

Nos estudos encontrados no Portal de Periódicos da CAPES, observa-se que vários autores assumem a definição de Governança de segurança da informação do ISACA (2015, p. 44, tradução nossa):

> Governança de segurança da informação é o subconjunto da governança corporativa que provê direção estratégica, garante que os objetivos serão atingidos, gerencia riscos apropriadamente, usa os recursos organizacionais com responsabilidade e monitora o sucesso ou falhas do programa de segurança institucional.

Moulton (2003) considera GovSI como sendo o estabelecimento e manutenção do ambiente para gerenciar os riscos relacionados com a confidencialidade, integridade e disponibilidade de informações e seus processos e sistemas de apoio, assim como a norma NBR ISO/IEC 27014:2013 (ABNT, 2013), Para Von Solms (2005), GovSI consiste na liderança, estruturas organizacionais, processo/procedimentos, aplicação da conformidade e mecanismos de monitoramento e tecnologias que garantem que a confidencialidade, integridade e disponibilidade dos ativos (em meios) eletrônicos da organização (dados, informações, *software* etc.) estejam sempre disponíveis e íntegros. Na mesma linha, considerando que GovSI abrange a confidencialidade, integridade e disponibilidade da informação, Sencioles (2012) e Manoel (2014) adotam o mesmo conceito em seus estudos.

Por outro lado, Williams (2001), em seu didático e abrangente trabalho sobre GovSI, traduz esta como sendo tudo que se refere à alta direção entender os riscos (decorrentes de segurança da informação) e às oportunidades de ganhos (positivos) pelo gerenciamento contínuo e apropriado destes riscos. Gestão de riscos também é defendida por Veiga (2007, p. 362), para o qual GovSI pode ser descrita como a maneira geral na qual informações de segurança são dispostas para mitigar riscos. Já para Johnston e Hale (2009) e Cabral e Caprino (2013, p. 177), GovSI consiste na liderança, na estrutura organizacional e em processos para proteção da informação, semelhante ao conceito adotado pelo DSIC (2008), que entende GovSI como o sistema pelo qual as atividades de segurança da informação de uma organização são dirigidas e controladas.

As publicações recentes utilizam como base as normas, conceitos e princípios da família das normas ISO/IEC 27000, ISO/IEC 38500, COBIT e NIST.

Com relação a modelos de governança de segurança da informação, Posthumus e Von Solms (2004) apresentam um *framework* de GovSI que se integra à governança corporativa. Partindo da descrição de informação corporativa, seu escopo, características, riscos, necessidades e importância, segregaram os requisitos de segurança da informação associados aos riscos da informação de negócios em internos e externos. O principal elo entre governança e gerenciamento são as políticas que mostram o compromisso da alta direção e dos gerentes executivos com segurança da informação, suportam a missão, objetivos e estratégia de

segurança da informação, bem como demonstram que há suporte ao estabelecimento e implementação de um amplo plano de segurança da informação.

Com a mesma base conceitual de Posthumus e Von Solms, Von Solms e Von Solms (2006) apresentam o modelo Ciclo Direção-Controle de GovSI. Eles partiram do conceito que qualquer modelo de governança deriva de um modelo de governança corporativa, sendo que este é sustentado por uma direção estratégica, caminho pelo qual a organização é conduzida, e se explicita à organização por meio de políticas, padrões da organização e procedimentos, e controle sobre todos os níveis de gerenciamento da organização, que é a conformidade com leis, normas e com as diretivas organizacionais. O ciclo direção-controle ocorre em todos os níveis de gerenciamento e consiste no núcleo da governança corporativa e, portanto, no núcleo de qualquer outro tipo de governança. Apesar das similaridades, os modelos diferem no nível de alcance na organização; enquanto Posthumus e Von Solms referem-se à governança como um dueto entre a alta gestão e o nível gerencial executivo, Von Solms e Von Solms entendem que a governança abrange todos os níveis, estratégico, tático e operacional.

Já o modelo apresentado por Da Veiga (2007) foi elaborado a partir da comparação de 22 elementos decompostos de quatro normas e trabalhos de GovSI: as Normas ISO/IEC 17799 e 27001 (2005), o Modelo *PROTECT* de Eloff (2005), o *CMM* de McCarthy e Campbell (2001) e o *ISA* de Tudor (2000). O modelo é concebido em quatro níveis, A, B, C e D, para tratamento de três componentes: estratégico, gerencial e operacional. Diferentemente dos modelos citados anteriormente, este modelo inova na medida em que introduz o tratamento da segurança da informação a partir de riscos identificados, considera o comportamento dos empregados como uma faceta da segurança da informação e enfatiza a necessidade de inserir, na cultura organizacional, a cultura de segurança da informação.

Na mesma linha de Eloff, Ula et al. (2011) apresenta um modelo de GovSI voltado ao sistema bancário baseado na comparação de 26 componentes, selecionados por serem princípios ou controles de segurança da informação, decompostos de sete normas e trabalhos de GovSI: Norma ISO/IEC 27002, o *Generally Accepted Information Security Principles* (*GAISP*) do *ISSA*, o COBIT 4.1, o modelo do *The Corporate Governance Task Force* (*CGTF*), o guia proposto pelo *The Corporate Information Security Working Group* (*CISWG*), o guia de auditoria do *The Federal Financial Institutions Examination Council* (*FFIEC*) e o *PCI Data Security Standard* (*PCI DSS*).

Por sua vez, Mellado et al. (2011) inovam ao analisarem nove *frameworks* de GovSI segundo os critérios de governança de Tecnologia da Informação (TI), governança corporativa, segurança da informação e adequação ao setor público, sendo que este último critério define a singularidade do estudo. O resultado da análise comparativa indica que a maioria dos modelos não detalha implicações específicas para implementação de GovSI em instituições públicas, sendo que somente o modelo do NIST considera as particularidades desse setor, contudo são necessários esforços para adaptar este modelo a leis e regras de outros países, uma vez que este modelo foi concebido segundo as leis e normas dos Estados Unidos da América.

A pequena quantidade de trabalhos desenvolvidos no Brasil encontrados nas pesquisas realizadas demonstra que o tema GovSI ainda é pouco explorado pela comunidade acadêmica. As pesquisas evidenciam, também, a pequena quantidade de material escrito direcionado às organizações públicas, evidenciando uma lacuna relevante na literatura que é a ausência de modelos de Governança de Segurança da Informação adequados à realidade da Administração Pública Brasileira.

3 METODOLOGIA DA PESQUISA

Dalfovo et al. (2008), em seu trabalho "Métodos quantitativos e qualitativos: um resgate teórico", explicita a classificação da pesquisa científica segundo os critérios de Ramos

et al. (2005), quais sejam, quanto à natureza e quanto à abordagem do problema. Quanto à natureza, esta pesquisa classifica-se como básica, pois pretende gerar um modelo conceitual de GovSI, e quanto à abordagem, qualitativa, uma vez que pretende verificar a relação da realidade com o objeto de estudo, cuja coleta de informações não é expressa em números, pois o que se busca é o entendimento do fenômeno como um todo, na sua complexidade, sendo a análise dos dados realizada indutivamente.

Para melhor compreensão, a pesquisa foi dividida em três fases. A primeira fase refere-se à pesquisa bibliográfica e à seleção de material para sustentação da pesquisa, o referencial teórico. Esta fase teve por objetivo realizar o levantamento das principais definições sobre governança de segurança da informação e comunicações e modelos existentes, por meio das normas e regulamentos brasileiros, artigos científicos, e publicações de entidades acreditadas no assunto como, por exemplo, o ISACA. A pesquisa foi feita pela Internet no sítio dos órgãos normatizadores/reguladores brasileiros e nos portais da CAPES e do Google Acadêmico. As práticas internacionais adotadas pelo setor público também foram pesquisadas na Internet.

A segunda fase consistiu na identificação dos elementos necessários a um modelo de governança de segurança da informação, baseado no referencial teórico adotado, e da construção de uma proposta de modelo com o viés do setor público brasileiro e, por fim, o desenho de sua representação gráfica. Nesta fase, se fez uso da norma ABNT NBR ISO/IEC 27014:2013 como pilar central, submetendo esta a uma customização textual face aos elementos identificados como necessários a um modelo para a APF. Esta customização fez uso de Análise de Conteúdo, sendo que, para a pesquisa, o método proposto por Bardin (1977) foi aplicado à norma NBR ISO/IEC 27014:2013 (ABNT, 2013), na estrutura proposta por Franco (2012) de categorias, sub-categorias, unidade de registro e de contexto.

A terceira fase consistiu na submissão da proposta de modelo de GovSI a um grupo focal formado por cinco especialistas da APF em SIC, tanto de nível gerencial quanto técnico, indicados pela Coordenação-Geral de Segurança da Informação (CGSIN) da STI/MPOG, que possuem direto e estreito relacionamento com os órgãos e entidades da APF e, ainda, fazem parte de uma unidade que possui assento no Comitê de Segurança da Informação do DSIC/GSI. A partir de suas observações, foi realizada a adequação do modelo proposto no que era pertinente ao objeto da pesquisa. A escolha da técnica de grupo focal justificou-se pela necessidade de utilização de um instrumento de pesquisa que favorecesse a livre expressão dos participantes à medida que refletissem e discutissem o tema proposto, permitindo, dessa forma, emergir os significados relacionados às questões apresentadas, decorrentes da experiência do grupo, na mesma linha de Gui (2003).

4 FUNDAMENTAÇÃO TEÓRICA

Para execução deste estudo foram selecionados os modelos de GovSI propostos pela ABNT e pelo NIST, uma vez que o primeiro é uma norma nacional atual sobre o tema e o segundo é um modelo originalmente desenhado para uso em instituições públicas. Foram também utilizadas as normas publicadas pelo DSIC/PR relacionadas ao tema.

4.1 Norma ABNT NBR ISO/IEC 27014:2013

Segundo a norma ABNT NBR ISO/IEC 27014:2013, a GovSI visa alinhar os objetivos e estratégias de segurança da informação com os objetivos e estratégias do negócio, sempre em conformidade com leis, regulamentos e contratos, adotando uma abordagem baseada em riscos para sua implementação e imputando ao corpo de governança da organização a responsabilidade pelas decisões e pelo desempenho. Os objetivos da GovSI são: alinhar os

objetivos e a estratégia da segurança da informação com os objetivos e estratégia do negócio (alinhamento estratégico); agregar valor para o corpo de governança e para as partes interessadas (entrega de valor); e garantir que os riscos da informação estão sendo adequadamente abordados (responsabilidade). Os resultados a serem atingidos com a implementação de GovSI, conforme preconizado em seu modelo, são: visibilidade para o corpo de governança sobre a situação da segurança da informação; uma abordagem ágil para a tomada de decisões sobre os riscos da informação; investimentos eficientes e eficazes em segurança da informação; e conformidade com requisitos externos (legais, regulamentares ou contratuais). Recomenda, também, que GovSI seja parte uma de uma visão holística e integrada de governança. Dentro dessa visão, os modelos de governança podem se sobrepor.

Para entregar valor às partes interessadas e garantir alinhamento entre segurança da informação e os objetivos do negócio, a norma estabelece seis princípios que fornecem uma base sólida para implementação de GovSI. A figura 1 apresenta o diagrama do modelo proposto com a interrelação dos processos avaliar, dirigir, monitorar e comunicar.

Figura 1 – Implementação do modelo de governança para a segurança da informação

Fonte: desenho adaptado da ABNT NBR ISO/IEC 27014:2013, página 6

É no processo avaliação que ocorre a ponderação sobre o alcance dos objetivos da implementação do modelo, considerando a situação prevista e a atual. O processo direção é onde o corpo de governança fornece o direcionamento sobre os objetivos e estratégias a serem implementadas. Na monitoração, por sua vez, é realizada a validação da eficácia das atividades de gerenciamento de SI, é assegurada a conformidade e se considera as alterações no ambiente de negócios. No processo comunicação, é realizada a troca de informações entre o corpo de governança e as partes interessadas de segurança da informação, é onde ocorre o reporte da situação de SI. Finalmente, a garantia é o processo pelo qual o corpo de governança solicita ou autoriza a realização de auditorias, que deverão realizar análises críticas ou certificações independentes e objetivas.

4.2 NIST 800-100

O National Institute of Standards and Technology (NIST), a partir do entendimento que segurança da informação é uma função essencial, publicou a norma NIST 800-100, Information Security Handbook: a Guide for Managers (NIST, 2007), que tem por finalidade informar aos membros das equipes de gerenciamento de segurança da informação sobre os vários aspectos

da segurança da informação que deverão ser implementados e supervisionados em suas organizações. Em seu capítulo 2, aborda o tema governança de segurança da informação.

A governança de segurança de informações em um departamento federal ou agência de governo norte-americano deve atender, no mínimo, aos requisitos exigidos em diretivas, regulamentos e legislação. Cada instituição deve adequar as suas práticas de governança de segurança de informação à sua missão, operação e necessidades.

Conceitualmente, o NIST define GovSI como o processo de estabelecer e manter um *framework* de governança de segurança da informação e de apoiar as estruturas de gestão e os processos para garantir que a segurança das informações estratégicas esteja alinhada com os objetivos de negócios, suporte esses objetivos, seja consistentes com as leis e regulamentações aplicáveis por meio da aderência a políticas e controles internos e proveja a atribuição de responsabilidades, tudo no esforço de gerenciar os riscos. As instituições públicas devem integrar suas atividades de GovSI com toda a estrutura e atividades da instituição, garantindo a participação adequada dos responsáveis pela instituição na supervisão da implementação dos controles de segurança de informações. As atividades-chave que facilitam essa integração são planejamento estratégico, estrutura organizacional, estabelecimento de regras e responsabilidades, integração com a arquitetura organizacional, e políticas e orientações de segurança da informação. A figura 2 apresenta os componentes da governança de segurança da informação definidos pelo NIST.

Figura 2 – Componentes da governança de segurança da informação

Fonte: diagrama adaptado da NIST Special Publication 800-100 (p. 6)

Para o NIST, a GovSI fornece uma estrutura para estabelecer e manter um programa de segurança de informações que irá evoluir com a instituição suportada.

4.3 Estudo comparativo de *frameworks* de GOVSI de Mellado et al. (2011)

No estudo realizado por Mellado et al. (2011) são comparados *frameworks* de GovSI à luz das especificidades e diferenciações naturais do setor público, identificando-se que a maioria dos *frameworks* avaliados podem ser utilizados por qualquer organização pública como ponto de partida para a integração de SI em seus processos, entretanto todos apresentam limitações e lacunas que precisam ser tratados para alcançar uma integração completa. Ponderam, ainda, que as instituições públicas também estão envolvidas nas discussões sobre falhas de segurança e possíveis vantagens competitivas alcançadas com alto grau de segurança, sendo que o alto grau de segurança em TI fortalece o relacionamento entre a administração pública e os cidadãos. Mellado et al. (2011) não encontraram na revisão de literatura realizada uma comparação abrangente e sistemática de modelos de GovSI, o que os

levou à elaboração de um conjunto de critérios de comparação selecionados de definições existentes de governança de segurança da informação, através da extração de características obrigatórias e desejáveis que cada *framework* deve possuir.

No que se refere às especificidades e diferenciações do setor público, os autores, não obstante concordarem que o setor público está sujeito às mesmas ameaças que as instituições privadas, consideram que o propósito de servir a sociedade e a obrigatoriedade de seguir estritamente o que está definido na legislação resultam em implementações de segurança diferenciadas de instituições privadas, uma vez que estas buscam atender os interesses de seus acionistas e podem suprir possíveis lacunas de legislação com interpretações que as beneficiem.

Dessa forma, os critérios de comparação utilizados foram:

a) Governança de TI, sob os cinco aspectos comumente explicitados nos *frameworks*:

- alinhamento estratégico: a segurança da informação precisa estar alinhada à estratégia de negócios para atingir os objetivos institucionais;

- entrega de valor ao negócio pela TI: os investimentos em TI devem promover a entrega dos benefícios prometidos aos negócios;

- gerenciamento do desempenho (da instituição) – deve haver o monitoramento das estratégias de segurança visando garantir o alcance dos objetivos institucionais, no tempo devido;

- gerenciamento de riscos: deve haver conscientização sobre riscos de segurança e a identificação de ameaças, vulnerabilidades e impactos para controlar e reduzir os riscos em toda a organização; e,

- controle e accountability: cada pessoa na instituição precisa estar envolvida nos controles de segurança e precisa conhecer suas responsabilidades no *framework* definido.

b) Governança corporativa, à luz de quatro domínios:

- objetivos institucionais: decisões estratégicas, desenvolvimento de políticas e orientações de segurança da informação, e os controles para monitorar se os objetivos institucionais estão sendo atingidos;

- processos: implementação e gerenciamento do processo de segurança da informação, com suas atividades e procedimentos;

- pessoas: estrutura organizacional. Definição de funções e responsabilidades das diferentes partes envolvidas; e

- tecnologia: a relação entre GovSI e os ativos físicos de TI que a instituição gerencia (internos e externos).

c) Segurança, devido à (óbvia) relação entre GovSI e segurança da informação, foram selecionados quatro critérios sobre o assunto:

- integração de normas: algumas propostas (dos *frameworks* analisados) referem-se aos controles e melhores práticas incluídas nas normas de segurança;

- gerenciamento de segurança da informação: algumas políticas e procedimentos definidos pela governança podem ser vinculados ao gerenciamento e ao lado operacional da segurança da informação;

- ferramentas e técnicas: normalmente *frameworks* utilizam ferramentas para facilitar sua implementação, tais como indicadores para medir o grau de conformidade ou modelos de maturidade para possibilitar benchmarking entre instituições; e

- orientações práticas para implementação: as abordagens teóricas podem se diferenciar das práticas, sem que esta envolvam detalhamento das atividades para implementação, incluindo casos de estudo e exemplos práticos.

d) Adequação ao setor público.

Embora todos os *frameworks* analisados possam ser adaptados ao setor público, alguns possuem algumas características que os tornam mais adaptáveis ao setor público. Esta

gama de particularidades varia desde a conformidade com leis, políticas e regulamentações originadas dos múltiplos órgãos de governo até limitações orçamentárias, de financiamento e de investimentos. Mellado et al. (2011 apud WIMMER; BREDOW, 2002) citam que as instituições públicas precisam considerar segurança para além dos aspectos técnicos, incluindo os domínios social, político, cultural e legal. Este quarto critério avalia estes domínios, visando ajudar a alta administração na decisão sobre o melhor *framework* de segurança da informação para uma instituição pública.

Segundo Mellado et al. (2011), a comparação realizada entre os diversos *frameworks* considerou três níveis de conformidade (baixo, médio, alto) para cada critério. Quanto à adequação ao setor público, segundo os autores, a maioria dos *frameworks* não detalha as implicações específicas da aplicação de GovSI em uma instituição pública. As diretrizes propostas pelo NIST são exceção, mas são fortemente aderentes às normas e legislação norte-americana, implicando em esforços adicionais na adaptação do *framework* em outros países. Todavia, ressaltam os autores, as instituições públicas, geralmente, estão submetidas a uma regulamentação específica e de diversos níveis, seja estadual ou nacional, seja pela natureza do setor em que a instituição está inserida, o que resulta em processos de governança diferentes, implicando na adaptação de qualquer modelo de GovSI a estas normas ou leis. Concluem Mellado et al. (2011) que nenhuma das abordagens abrange todos os requisitos que uma instituição pública precisa atender, embora possuam características desejáveis, suas principais lacunas foram ressaltadas no estudo realizado. Os autores concluem que a maioria dos modelos são mais voltados ao setor privado, fato que deve ser considerado pelos gestores de instituições públicas, quando da sua adoção. O Quadro 1 sintetiza as comparações realizadas por Mellado et al. (2011).

Quadro 1 – Comparação dos *frameworks* de GovSI

Framework / **Critério**	**Guia prático de GovSI**	**BSA**	**Políticas de SI**	**GovSI (modelo Von Solms)**	**ISACA**	**ISO**	**ITGI**	**NIST**	**SEI**
Governança de TI									
Alinhamento Estratégico	Médio	Médio	Alto	Médio	Alto	Médio	Alto	Alto	Alto
Entrega de valor ao negócio pela TI	Médio	Baixo	Baixo	Baixo	Médio	Baixo	Alto	Baixo	Médio
Gestão de desempenho	Baixo	Médio	Médio	Médio	Médio	Alto	Alto	Médio	Baixo
Gestão de riscos	Alto	Alto	Alto	Alto	Baixo	Alto	Alto	Alto	Alto
Controle e *Accountabili-ty*	Médio	Baixo	Médio	Alto	Baixo	Médio	Alto	Baixo	Alto
Governança Corporativa									
Objetivos Institucionais	Médio	Médio	Alto	Médio	Alto	Médio	Alto	Alto	Alto
Processos	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
Pessoas	Alto	Alto	Baixo	Alto	Alto	Médio	Médio	Alto	Médio

Tecnologia	Alto	Baixo	Médio	Médio	Alto	Médio	Baixo	Baixo	Médio
Segurança									
Integração de normas	Alto	Médio	Baixo	Alto	Baixo	Alto	Baixo	Alto	Médio
Gestão de segurança da informação	Médio	Baixo	Médio	Alto	Baixo	Alto	Médio	Médio	Médio
Ferramentas e técnicas	Alto	Alto	Médio	Baixo	Baixo	Alto	Médio	Baixo	Baixo
Orientações práticas para implemen-tação	Médio	Alto	Baixo	Médio	Médio	Alto	Baixo	Médio	Médio
Adequabilidade ao setor público	Baixo	Médio	Baixo	Baixo	Baixo	Baixo	Baixo	alto	Baixo

Fonte: desenho adaptado de Comparative Analysis of Information Security Governance *Frameworks*: A Public Sector Approach, Mellado et al., Conference Paper, Junho de 2011. Disponível em: http://www.researchgate.net/publication/232252326. Acesso em: 8 de Mai. 2015

4.4 Normas Brasileiras

O DSIC, órgão da Presidência da República, é responsável por SIC na APF. As normas emanadas desse órgão regulam as questões de segurança da informação na APF e são fiscalizadas, quanto ao seu cumprimento, pelo TCU. Para a pesquisa foram utilizadas as seguintes normas:

- Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 - disciplina a gestão de segurança da informação e comunicações na APF.

- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008 - define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da APF.

- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 30 de junho de 2009 - estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da APF.

- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013 - estabelece diretrizes para o processo de gestão de riscos de segurança da informação e comunicações – GRSIC nos órgãos ou entidades da APF.

- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009 – disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da APF.

- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 30 de janeiro de 2012 - estabelece diretrizes para o processo de inventário e mapeamento de ativos de informação, para apoiar a SIC dos órgãos e entidades da APF.

- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 30 de janeiro de 2012 - estabelece diretrizes para avaliação de conformidade nos aspectos relativos à SIC nos órgãos ou entidades da APF.

- Portaria CDN n° 14 (CDN, 2015), de maio de 2015, em atenção à recomendação do Acórdão 3.051/2014-TCU-Plenário e de forma complementar à Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, apresenta a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0. A estratégia de SIC e a SegCiber, base da Defesa Cibernética, visam assegurar o uso

do espaço cibernético, impedindo ou dificultando, em seu âmbito, ações contra os interesses do País e da sociedade e têm a finalidade de apresentar diretrizes estratégicas para o planejamento de segurança da informação e comunicações e de segurança cibernética no âmbito da APF, objetivando a articulação e a coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo Brasileiro e a mitigação dos riscos aos quais encontram-se expostas as organizações e a sociedade. As diretrizes da Estratégia aplicam-se a todos os órgãos e entidades que integram a APF.

5 BASE DA PROPOSTA DE MODELO DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Considerando o referencial teórico e a necessidade da APF de atender os requisitos legais emanados dos órgãos normatizadores, a proposta de modelo de GovSI para APF foi construída em quatro etapas. A primeira etapa consistiu na identificação dos elementos de GovSI presentes nas normas publicadas pelo DSIC. Na segunda etapa, foram confrontados os elementos de GovSI identificados na primeira etapa com os critérios definidos por Mellado et al. (2011). Na terceira etapa, a norma ABNT NBR ISO/IEC 27014:2013 foi avaliada quanto à sua aderência aos critérios de Mellado et al. (2011), de forma similar ao realizado na segunda etapa. A quarta etapa foi a combinação dos modelos a partir da seleção do modelo de mais alta aderência identificado na comparação realizada na terceira etapa. A comparação realizada entre a norma e os modelos considerou três níveis de conformidade (baixo, médio, alto) para cada critério. O Quadro 2 representa essa combinação, permitindo a visualização do modelo mais aderente ao critério.

Quadro 2 – Comparação do modelo do NIST, das normas DSIC e do modelo ABNT com os critérios de avaliação

Modelo/Normas / **Critérios**	**NIST**	**DSIC**	**ABNT**
Governança de TI			
Alinhamento estratégico	Alto	Baixo	Alto
Entrega de valor ao negócio pela TI	Baixo	N. A.	Alto
Desempenho do gerenciamento (da instituição)	Médio	Alto	Alto
Gerenciamento de riscos	Alto	Alto	Alto
Controle e *accountability*	Baixo	Médio	Médio
Governança Corporativa			
Objetivos institucionais	Alto	Alto	Alto
Processos	Alto	Alto	Baixo
Pessoas	Alto	Médio	Alto
Tecnologia	Médio	Alto	Alto
Segurança			
Integração de normas	Alto	Baixo	Médio
Gerenciamento de segurança da informação	Médio	Baixo	Alto
Ferramentas e técnicas	Baixo	Baixo	Baixo
Orientações práticas para implementação	Médio	Médio	Baixo
Adequação ao setor público	Alto	Alto	Alto

Fonte: Os Autores

*N.A. – não se aplica

Para seleção do modelo mais aderente ao critério, foi utilizado, por similaridade, o método de votação winner-takes-all, onde o mais alto grau é o selecionado. No caso de mesma classificação, utiliza-se o critério de desempate da primazia das normas do DSIC sobre as

demais, uma vez que as instituições da APF são obrigadas a seguir essas normas. Persistindo o empate, ou no caso dos modelos ABNT e NIST possuírem maior aderência ao critério do que as normas do DSIC, foi dada prioridade de seleção ao modelo proposto pela ABNT. Esta prioridade deve-se ao fato de o modelo da ABNT ser reconhecido como "boa prática" pelos órgãos fiscalizadores da APF e por ser uma norma reconhecida no mercado brasileiro.

Como pode ser observado, o modelo a ser elaborado deve ser resultado da combinação harmônica de vários elementos constantes do referencial adotado.

6 PROPOSTA DE MODELO DE GOVSI

Via de regra, as normas do DSIC estabelecem diretrizes, critérios, procedimentos e metodologias, sendo aplicadas no âmbito da Administração Pública Federal, direta e indireta. O modelo de GovSI proposto pela ABNT aplica-se a todos os tipos e tamanhos de organizações, não contrariando o disposto nas normas do DSIC. Considerando o objetivo desta pesquisa, o escopo do modelo proposto será a Administração Pública Federal, direta e indireta, e fornecerá orientações, conceitos e princípios para a GovSI, à luz do disposto na Estratégia. Além disso, os conceitos a seguir apresentados são originários da norma ABNT NBR ISO/IEC 27014:2013, portanto com representação similar e seguindo o mesmo padrão disposto na norma, porém, com as devidas adaptações à APF.

6.1 Conceitos

A GovSI visa alinhar os objetivos de segurança da informação e comunicações com as diretrizes e objetivos estratégicos dos órgãos e entidades que integram a APF, aprimorando a SIC por meio da mitigação dos riscos aos quais está exposta, assegurando e defendendo os interesses do Estado e da sociedade. Este conceito é aderente aos objetivos estratégicos: OE-I, 5° parágrafo, OE-IV, 3° parágrafo, OE-V, todo, OE-VIII, todo e OE-IX, 4° parágrafo da Estratégia.

Compete ao Gabinete de Segurança da Informação – GSI operacionalizar as diretrizes, estratégias, normas, orientações e todo o arcabouço conceitual que sustente a implementação de uma sistemática de gestão de SIC pelos órgãos e entidades da APF, direta e indireta. Compete, ainda, ao GSI, avaliar, dirigir, monitorar, garantir e comunicar sobre essa implementação. As responsabilidades do chefe do GSI são indelegáveis, sendo este responsabilizado por erros ou falhas na implementação da sistemática de GovSI nacional e de gestão de SIC na APF. O chefe do GSI, para exercer suas competências, deve deliberar sobre as diretrizes, estratégias, normas, orientações e o que mais for necessário à sistemática de gestão de SIC na APF, em conjunto com as mais altas autoridades da APF, que compõem o Comitê Gestor de SIC da APF. A mais alta autoridade de cada instituição da APF é responsável por garantir a implementação de uma sistemática de SIC eficiente, eficaz, aceitável e em conformidade com as leis e normas, alinhada com os objetivos e estratégias institucionais, e que assegure a implantação de políticas públicas que atendam as expectativas do Estado e da sociedade. A mais alta autoridade de cada instituição pode delegar a responsabilidade pela implementação da sistemática de SIC, porém a responsabilização de incidentes decorrentes de erros ou falhas na implementação permanece sob sua competência. As competências estão aderentes ao objetivo institucional OE-IV, em especial ao 2° parágrafo, que estabelece a competência de coordenação do GSI, e ao 4° parágrafo no que tange os demais órgãos da APF, sendo, em ambos os casos, aprimorados no que tange a "*accountability*".

6.2 objetivos

Os objetivos da GovSI são: a) alinhar os objetivos e estratégia da SIC com os objetivos e estratégias das instituições e órgãos que compõem a APF; b) agregar valor para a APF, para o Estado e para a sociedade; e c) garantir que os riscos da informação estão sendo adequadamente mitigados.

Esses objetivos estão alinhados ao referencial estratégico da Estratégia, páginas 37 a 54.

6.3 Resultados esperados

Os resultados a serem alcançados com a implementação da GovSI são: a) visibilidade sobre a situação de SIC na APF; b) agilidade das tomadas de decisões quanto os riscos da informação; c) redução de custos e investimentos eficientes e eficazes em SIC; e, d) conformidade legal.

Os resultados esperados estão alinhados ao resultado esperado da Estratégia, descrito no 2° parágrafo, linha 10, página 34, qual seja, a articulação e a coordenação de esforços dos diversos atores envolvidos, uma vez que essas contribuições da academia para o aprimoramento de SIC no Governo primaram pela interação constante com os diversos atores envolvidos no tema.

6.4 Princípios

A articulação e a coordenação de esforços entre os diversos órgãos e entidades que compõem a APF é condição indispensável à proteção das informações das organizações e da sociedade. Os princípios aqui expostos visam obter o alinhamento necessário da segurança da informação com as estratégias de Estado, por meio de GovSI, e entregar valor às partes interessadas, quais sejam, o próprio Estado e a sociedade. Os princípios são a base para a implementação do processo de GovSI, sendo genéricos o suficiente para abarcar toda a APF com suas diversas particularidades, porém específicos o bastante para contemplar as suas características comuns. O sucesso desse modelo de GovSI depende da aceitação, pela mais alta autoridade de cada instituição da APF, das responsabilidades e responsabilizações inerentes à sua implementação.

- Princípio 1: Aprimorar a segurança da informação em toda a APF.

A GovSI deve garantir que as atividades de SI dispostas na legislação e nas normas publicadas pelo GSI sejam entendidas e internalizadas em todos os órgãos e entidades da APF. A tomada de decisão nessas instituições deve considerar a política pública, a SIC e os demais aspectos relevantes à sua consecução. As ações de segurança física e lógica referentes à infraestrutura crítica de informações devem ser rigorosamente coordenadas. A POSIC de cada órgão e entidade da APF deve prever as responsabilidades e responsabilizações de cada atividade de SIC executada. A GovSI deve tomar decisões baseadas em riscos, devendo ser definido o grau aceitável de exposição a riscos. Este princípio está diretamente relacionado ao objetivo estratégico OE-IX.

- Princípio 2: Estabelecer uma estratégia de investimento

A GovSI deve promover o planejamento dos investimentos em SIC, priorizando o fortalecimento das ações cooperativas entre as instituições públicas e, quando possível, entre essas e as instituições privadas. O planejamento deve prever as necessidades atuais e futuras de SIC e estar alinhado ao PPA. Este princípio atende ao disposto nos objetivos estratégicos OE-I e OE- IX, 3° parágrafo.

- Princípio 3: Manter a conformidade legal

A GovSI deve assegurar que a POSIC e as ações de gestão de SI de cada instituição da APF cumpram o estabelecido em leis e normas nacionais e que atendam a requisitos

contratuais internos e externos. A sistemática de gestão de SI dos órgãos e entidades da APF deve ser item obrigatório e permanente na avaliação de conformidade realizada pelas unidades de controle interno de cada instituição e pelos órgãos externos de fiscalização e controle. Este princípio atende ao disposto no objetivo estratégico OE-VII, 4° parágrafo.

- Princípio 4: Desenvolver a cultura de SIC

A GovSI deve estimular a educação e conscientização da importância de SIC, promovendo, assim, mudanças comportamentais, de pessoas e das instituições, de forma a obter uma postura humana responsável e consciente, e elevar o grau de maturidade das instituições. A GovSI deve considerar que o comportamento humano é essencial para o alcançamento dos níveis de segurança desejados, portanto os objetivos, papéis, responsabilidades e responsabilizações devem ser explicitamente divulgados e conhecidos. Este princípio se relaciona aos objetivos estratégicos OE-VII e OE-X.

- Princípio 5: Estabelecer ações colaborativas

A GovSI deve promover a articulação e o desenvolvimento de parcerias entre as instituições públicas e privadas, visando o desenvolvimento dos profissionais de SIC da APF, a adoção de boas práticas, novas soluções tecnológicas e de estímulo ao desenvolvimento de novos produtos e serviços que aprimorem a SIC. Este princípio atende ao disposto nos objetivos estratégicos OE-II, OE-III e OE-VI.

Princípio 6: Monitorar o desempenho da segurança

A GovSI deve garantir que as ações de proteção das informações sejam adequadas e que mantenham os níveis acordados de SI. O monitoramento deve ser holístico, contínuo, buscando identificar o desempenho da SI em relação: a seu apropriado suporte às ações previstas no planejamento estratégico institucional; ao impacto nas políticas públicas e, por consequência, na sociedade; à aderência das políticas processos e procedimentos existentes às novas tecnologias, ambiente externo e interno, e políticas públicas; à efetividade, eficácia e eficiência dos controles de segurança. Este princípio atende ao disposto nos objetivos estratégicos OE-I, OE-IV,OE-VII e OE-VIII.

6.5 Processos

Em atendimento ao OE-IV, para estabelecer a GovSI os atores envolvidos devem executar os seguintes processos:

Processo Avaliação - este processo consiste em avaliar se estão sendo atingidos os objetivos de SI, promovendo a correção de possíveis ajustes necessários, de forma a garantir que os objetivos sejam efetivamente alcançados. Os responsáveis pela GovSI devem assegurar que as políticas públicas considerem os aspectos de SI.

Processo Direção - processo por meio do qual o GSI apresenta o direcionamento dos objetivos e estratégias de SIC que precisam ser implementados. O direcionamento pode incluir alterações em recursos, nos planos de gestão de riscos, na priorização de atividades e políticas, e na aceitação de riscos.

Processo Monitoração - este processo prevê a validação do alcançamento dos objetivos estratégicos de SIC e sua agregação de valor. Para realizar este processo, a GovSI deve avaliar a eficácia do modelo de gerenciamento de SIC das instituições, a sua conformidade com os requisitos internos e externos, e as alterações de cenários, internos e externos, de leis e regulamentos, e o potencial impacto desses sobre os riscos de informação.

Processo Comunicação - neste processo se dá a troca de informações com as partes interessadas, governo e sociedade, sobre os objetivos de SI e as ações de SIC implantadas. Para executar este processo, a GovSI deve: comunicar à sociedade que a APF pratica um nível de segurança da informação compatível com o requerido pelas políticas públicas; notificar os órgãos e entidades da APF sobre a necessidade de ações corretivas em questões de SIC; e

identificar as expectativas com relação a SIC da sociedade, do governo, do Estado e das políticas públicas.

Processo Garantia - Este processo consiste no relacionamento com os órgãos de controle e auditoria da APF, os quais encaminham relatórios onde são identificadas e validadas as ações para elevação do grau de maturidade de SIC bem como a avaliação das próprias ações e decisões tomadas no âmbito da GovSI da APF. Para executar este processo, a GovSI deve firmar parceria com os órgãos de controle e auditoria da APF e com as autoridades da APF, apoiando os trabalhos realizados por aqueles.

7 AVALIAÇÃO DO MODELO DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PELO GRUPO FOCAL

O modelo proposto foi submetido à avaliação de um grupo focal formado por cinco especialistas em segurança da informação e comunicações, tanto de nível gerencial quanto técnico, e que possuem direto e estreito relacionamento com os órgãos e entidades da APF e, ainda, fazem parte de uma unidade que possui assento no Comitê de Segurança da Informação do DSIC/GSI. Para a realização da avaliação do modelo proposto, foram elaboradas três questões básicas, visando estimular o debate, quais sejam:

Questão 1 - O modelo proposto, baseado na ABNT NBR ISO/IEC 27014:2013, atende às normas e recomendações do GSI?

Questão 2 - O modelo proposto está aderente à Estratégia?

Questão 3 - O modelo proposto reflete a sua visão de Governança de Segurança da Informação e Segurança Cibernética?

Analisando o modelo, o que inicialmente chamou a atenção do grupo foi o *lócus* onde está vinculado o Comitê Gestor. Na sequência, foi colocada a questão do arranjo institucional, onde, segundo os participantes, a estruturação deve ser sistêmica, ou seja, ordenada para que todos os órgãos e entidades da APF a cumpram, facilitando os controles. Em linhas gerais, inicialmente, o modelo foi considerado "inibido", todavia representa a visão atual do Estado, que, de uma visão estratégica existente há alguns anos, passou para uma visão militarizada, no que tange à SIC. Foi ressaltado também o entendimento que segurança cibernética é um subconjunto de SIC, sendo essa formada por três eixos: o crime, a segurança e a defesa cibernética. Foi também inserida a questão da necessidade de orçamento específico, único, para SIC na APF, evitando sua fragmentação e pulverização, propiciando padronização e um modelo sustentável, alinhando SIC a outros temas de Estado. Foi citada a questão da conscientização e educação para SIC como muito importante.

Especificamente, quanto à questão 1, um dos participantes afirmou que não conseguia perceber a vinculação das normas DSIC à norma ABNT, porque, no seu entendimento, as normas do GSI são processos de trabalho que devem ser implantados nos órgãos da APF, sendo o modelo proposto a arquitetura que daria suporte à implantação desses processos de trabalho. Todavia, para implantação do modelo, seria necessária a alteração das competências do DSIC, pois o Decreto 8.577, de 26/11/2015, alterou a estrutura da Presidência da República e as competências do DSIC.

Quanto à segunda questão, afirmou-se que o modelo merece ser prospectado, todavia é necessário, para que este, ou qualquer outro modelo, funcione, que existam profissionais capacitados que o sustentem. Outra ponto relevante apresentado foi que o arcabouço de normas do GSI é adequado, porém falta uma arquitetura que propicie sua implementação; o modelo proposto pode servir a esse fim. Na análise realizada pelos participantes, o modelo está aderente à Estratégia.

Quanto à questão 3, os participantes concordaram que o modelo reflete suas visões de GovSI, com exceção de um participante que considera como modelo ideal o de entidade única

(agência reguladora estatal), que direcionaria, de forma exclusivamente técnica, as questões de SIC na APF. Por fim, foi ressaltada a importância da autonomia do Comitê Gestor e, como fator crítico de sucesso para a implantação de um modelo de GovSI, o viés político.

CONSIDERAÇÕES SOBRE A AVALIAÇÃO DO MODELO

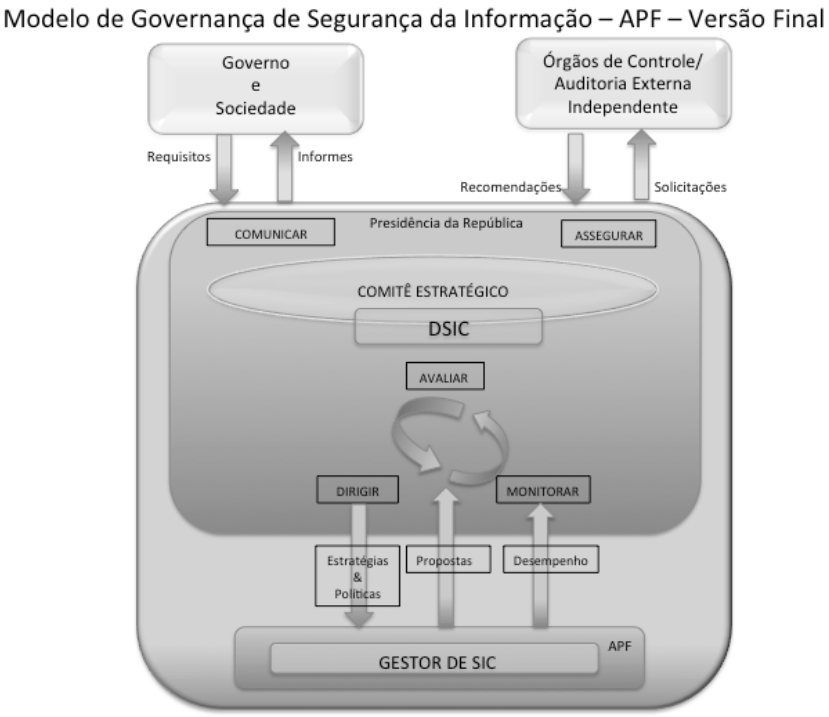
Como pode ser observado, as contribuições do grupo focal foram significativas para melhorias do modelo proposto. As preocupações quanto ao fracionamento de SIC na APF, a falta de representatividade do Comitê Gestor atual, a falta de orçamento próprio, a redução da visão estratégica, a necessidade de um posicionamento adequado na estrutura do Estado, dentre outras, podem ser abordadas com o modelo proposto, desde que exista, de fato, o entendimento, pela alta administração do Poder Executivo, da relevância e urgência do tema.

O Decreto 8.577, de 26/11/2015, alterou a estrutura regimental da Presidência da República e as competências do DSIC, entretanto, sem avaliação de mérito, o DSIC continua responsável por SIC na APF, conforme observado no artigo 9° do Decreto.

A ideia de uma agencia reguladora ser a direcionadora de SIC na APF, valendo-se de comitê ou comitês, com participação mista de agentes militares e da sociedade civil, extrapola o objeto deste pesquisa, contudo, ainda que seja uma alternativa que venha a ser implementada pelo Governo Federal, esta deverá possuir um modelo de GovSI para efetividade de sua atuação.

Desta forma, analisando as ponderações e acolhendo algumas sugestões do grupo focal, o modelo proposto, em versão final, é o apresentado na Figura 3.

Figura 3 – Versão final do Modelo de Governança de Segurança da Informação para a APF



Fonte: os autores

A principal alteração do modelo em relação ao modelo originalmente proposto ocorreu no Comitê Gestor, que passa a ser o principal *lócus* de deliberação das estratégias, diretrizes e orientações de SIC para a APF, em contraponto à visão inicial onde era uma instância de assessoramento e de caráter opinativo. Renomeado para Comitê Estratégico para melhor compreensão de seu papel, mantém, para que sejam efetivas suas ações, a exigência

de que seus representantes sejam altas autoridades da APF, ministros de Estado ou representantes diretamente a eles vinculados, ou secretários executivos, ou seja, autoridades com elevado poder decisório. O entendimento do grupo focal sobre a necessidade da CGU e da AGU serem membros deste Comitê não foi acatada, uma vez que poderia haver conflito de interesses no caso do primeiro, por ser órgão de controle, e a obrigatoriedade de parecer da AGU para a emissão de qualquer ato normativo ou regulador, no caso do segundo. Ressalta-se que o Comitê Estratégico pode convocar qualquer dos órgão citados para participação eventual nas reuniões, caso entenda necessário.

8 CONCLUSÃO

Na revisão da literatura realizada, foram identificados vários modelos de GovSI, elaborados por pesquisadores estrangeiros, de uso geral, que podem ser utilizados em qualquer tipo de organização. Todavia, somente uma proposta, a do NIST, era direcionada ao setor público. Um estudo realizado por pesquisadores espanhóis, Mellado et al (2011), comparou *frameworks* de GovSI, incluindo entre os critérios de comparação a adequabilidade ao setor público.

Para a construção de um modelo de GovSI aderente à Estratégia, foram avaliados o modelo NIST, porque este modelo é destinado ao setor público, a norma ABNT NBR ISO/IEC 27014:2013, uma vez que esta é uma norma aceita no mercado nacional, e as normas publicadas pelo DSIC, de cumprimento obrigatório pela APF.

O modelo de GovSI proposto apresenta as características de integração à governança corporativa descritas no modelo de Posthumus e Von Somls (2004), aos principais elementos do modelo de Da Veiga (2007), e é, ainda, aderente ao preceito de níveis estratégico, tático-operacional e técnico, do modelo de Ula et al (2011). Em contraposição, o modelo proposto não é aderente ao modelo apresentado por Von Solms e Von Solms (2006), uma vez que este considera que um modelo de GovSI deve ser derivado de um modelo de governança corporativa. A não aderência a este modelo se justifica pelo fato de não haver um modelo de governança corporativa único para toda a APF, tendo cada órgão ou entidade seu próprio sistema de governança corporativa, conforme pode ser depreendido do trabalho de Britto (2011).

Considerando a crescente utilização de soluções de TIC pelos Estados e pela sociedade e, paralelamente, o crescimento das ameaças e vulnerabilidades neste ambiente e, ainda, as fragilidades existentes nos processos e o baixo nível de maturidade de gestão de SIC na APF, o estabelecimento de uma governança de segurança da informação adequadamente estruturada passa a ser condição indispensável à sustentabilidade das políticas públicas e à melhor prestação de serviços ao cidadão.

Esta pesquisa se propôs apresentar um modelo de GovSI para a APF, considerando as restrições e requerimentos legais e normativos existentes e as características inerentes ao setor público, portanto, entende-se que foi atingido o objetivo geral e os objetivos específicos apresentados, uma vez que o modelo proposto foi submetido à avaliação de um grupo focal formado por especialistas da APF em SIC, sendo considerado adequado à realidade atual da APF.

A pesquisa tem como limitações o fato de apresentar um modelo conceitual, que não foi implementado para teste de sua viabilidade e de sua efetividade. Apresenta-se também como limitador o fato de não ter sido submetida ao GSI e ao Comitê da APF que o assessora, nem às altas autoridades da APF, para avaliação, críticas e discussão desses atores sobre o modelo, considerando que estes exercem atividades essenciais para o sucesso de GovSI na APF.

Sugere-se como trabalhos futuros: a elaboração de um *framework* de SIC para a APF, integrando em um modelo a governança e a gestão de SIC; um modelo de maturidade em GovSI para as organizações da APF; um estudo sobre delimitação de foco de atuação de SIC e Segciber no Brasil; uma proposta sobre como inserir na cultura corporativa existente na APF os elementos requeridos de SIC; e um estudo aprofundado para elaboração de um modelo de governança corporativa para a APF brasileira.

Por fim, entende-se que a maior contribuição dessa pesquisa foi estimular a discussão sobre Governança de Segurança da Informação e Comunicações na Administração Pública Federal brasileira, em atendimento aos objetivos estratégicos OE-III e OE-VI da Estratégia.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27014:2013. Técnicas de segurança — Governança de segurança da informação. 2013.

BRITTO, T. D.; Neto, J. S. **Levantamento e diagnóstico de maturidade da governança da segurança da informação na administração direta federal brasileira**. Universidade Católica de Brasília. 2011. Disponível em: http://www.bdtd.ucb.br/tede/tde_busca/arquivo.php?codArquivo=1429. Acesso em: 20 Jun. 2015.

CABRAL, C.; CAPRINO, W. **Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados**. Ebook. Editora Brasport, 2015.

CDN. Portaria nº 14, de 11 de maio de 2015, **Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0**", desdobramento da Instrução Normativa GSI/PR nº 01/2008. Disponível em: http://www.gsi.gov.br/arquivos/portaria-dsic.pdf. Acesso em: 11 mai. 2015.

DA VEIGA, A.; ELOFF, J. H. P. **An Information Security Governance Framework**. Information Systems Management, 24:4, p. 361-372, 2007. Disponível em: URL: http://dx.doi.org/10.1080/10580530701586136. Acesso em: 30 Ago. 2015.

DALFOVO, M. S.; LANA, R. A.; SILVEIRA, A. Métodos quantitativos e qualitativos: um resgate teórico. **Revista Interdisciplinar Científica Aplicada**, Blumenau, v. 2, n. 4, p. 1- 13, Sem II. 2008. Disponível em: http://www.unisc.br/portal/upload/com_arquivo/metodos_quantitativos_e_qualitativos_um_resgate_teorico.pdf. Acesso em: 30 Abr. 2016.

DSIC. **Instrução Normativa GSI/PR nº 1**, de 13 de junho de 2008. Disponível em: http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf. Acesso em: 06 Jun. 2015. (Brasil, 2013).

ELOFF, J. H. P.; ELOFF, M.M. **Information security architecture**. Computer Fraud & Security, v. 5, n. 11, p. 10-16, 2005. Disponível em: http://www.sciencedirect.com/science/article/pii/S136137230570275X. Acesso em: 30 Ago. 2015.

FRANCO, M. L. P. B. **Análise de Conteúdo**. 4. ed. Brasília: Liber Livro, 2012.

GUI, R. T. Grupo focal em pesquisa qualitativa aplicada: intersubjetividade e construção de sentido. **Rev. Psicol. Organ. Trab**., v. 3, n. 1, p. 135-159, jun. 2003. Disponível em: http://pepsic.bvsalud.org/pdf/rpot/v3n1/v3n1a07.pdf. Acesso em: 02 Abr. 2016.

ISACA. Glossário. 2015. Disponível em: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. Acesso em: 06 Jun. 2015.

JOHNSTON, A.C.; HALE, R. Improved Security through Information Security Governance. **Communications of the ACM**, v. 52, n. 1, jan. 2009. Disponível em: https://www.researchgate.net/publication/220420549_Improved_Security_through_Information_Security_Governance. Acesso em: 30 Ago. 2015.

MANOEL, S. S. **Governança de Segurança da Informação:** Como criar oportunidades para o seu negócio. Brasport, 2014.

MELLADO, D., CRESPO, L. E. S., REBOLLO, O., FERNÁNDEZ-MEDINA, E. **Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach**. Conferência: 11th European Conference on e-Coverment (ECEG'11), Ljubljani, Slovenia, dias 16 e17 de Junho de 2011, p. 482-490. Disponível em: http://www.researchgate.net/publication/232252326 . Acesso em: 30 Ago. 2015.

MOULTON, R.; COLES, R.S. Applying information security governance. **Computers & Security**, v**.** 22, n. 7., 2003.

NIST. **Information Security Handbook:** a Guide for Managers. 2007. Disponível em:http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Acesso em 20 Jun 2015.

POSTHUMUS, S.; VON SOLMS, R. A framework for the governance of information security. **Computers & Security**, 23, p. 638-646, 2004. Disponível em: http://www.sciencedirect.com/science/article/pii/S0167404804002639. Acesso em: 30 Mai. 2015.

SENCIOLES, S. V. O. **Proposta de critérios para avaliação da segurança da informação de uma organização**. 2011. 56 f. Trabalho de Conclusão de Curso (Especialização) – Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/handle/1/420. Acesso em: 13 Jul. 2015.

ULA, M.; ISMAIL, Z.B.; SIDEK, Z.M. A Framework for the Governance of Information Security in Banking System. **Journal of Information Assurance & Cybersecurity**, Disponível em: http://www.ibimapublishing.com/journals/JIACS/2011/726196/a726196.html. Acesso em 30 ago. 2015.

VEIGA, A.; ELOFF, J. H. P. An Information Security Governance Framework. **Information Systems Management**, v. 24, n. 4, p. 361-372. 2007. Disponível em: http://dx.doi.org/10.1080/10580530701586136. Acesso em 13 jun. 2014.

VON SOLMS, S. H. B. Information Security Governance e Compliance management vs operational management. **Computers & Security**, v. 24, p. 443-447, set. 2005. Disponível em:

http://www.sciencedirect.com/science/article/pii/S0167404805001057. Acesso em: 30 mai. 2015.

VON SOLMS, R.; VON SOLMS, S. H. B. Information Security Governance: A model based on the Direct–Control Cycle**. Computers & Security**, v. 25, Issue 6, p. 408-412, Set. 2006. Disponível em: http://www.sciencedirect.com/science?_ob=ArticleListURL&_method=list&_ArticleListID=-993282952&_sort=r&_st=4&md5=4bee1a5aa2112897b716bbb9d3201b9b&searchtype=a. Acesso em: 30 mai. 2015.

WILLIAMS, A. P. Information Security Governance. **Information Security Technical Report**, v. 6, n. 3, p. 60-70, 2001. Disponível em: http://www.sciencedirect.com/science/article/pii/S1363412701003090. Acesso em: 20 jul. 2015.

Artigo recebido em 05/06/2017 e aceito para publicação em 30/11/2018