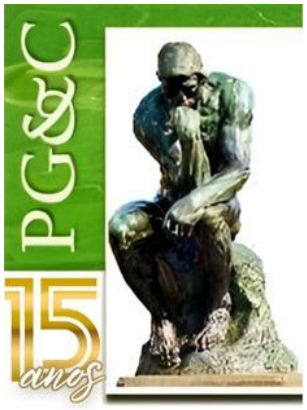
RELATOS DE PESQUISA



APLICAÇÃO DE UM MODELO DE MATURIDADE EM GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL

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

João Souza Neto
Doutor em Engenharia Elétrica pela Universidade de Brasília, Brasil.
Professor da Universidade de Brasília, Brasil.
E-mail: szneto@gmail.com

Tomás Roberto Cotta Orlandi
Doutor em Ciência da Informação pela Universidade de Brasília, Brasil.
Analista Sênior da Empresa Brasileira de Correios e Telégrafos, Brasil.
E-mail: tomasroberto@gmail.com

Resumo
Este artigo propõe um modelo para a Governança de Segurança da Informação para a Administração Pública Federal para ser aplicado em qualquer órgão público. Esta pesquisa tem por objetivo geral propor a aplicabilidade, em relação aos níveis de maturidade, do modelo de Governança de Segurança da Informação e Comunicações. O modelo apresentado está em concordância com os princípios de Segurança da Informação, às leis e aos regulamentos pertinentes e, ainda, à boa governança corporativa das entidades públicas. Ao ser aplicado o modelo na organização, é possível identificar o estágio de maturidade de Governança de Segurança da Informação na instituição, indicar os pontos que precisam ser melhorados e, ainda, fazer uma comparação com outras instituições que aplicarem o referido modelo. Quanto à metodologia, consiste em uma pesquisa descritiva que utiliza técnicas padronizadas de coleta de dados, nas quais o modelo é analisado por meio das respostas dos respondentes às perguntas formuladas sobre a pertinência dos conceitos abordados no referido modelo. Além disso, também é uma aplicação prática que procurou validar a construção do modelo citado. Como resultados tem-se a possibilidade de avaliar a maturidade em segurança da informação da organização, a evolução da maturidade ao longo do tempo e a possibilidade de compara com outras organizações que também aplicarem modelo.

Palavras-chave: governança de segurança da informação; modelo de maturidade; framework; administração pública.

APPLICATION OF A MATURITY MODEL IN INFORMATION SECURITY GOVERNANCE FOR THE FEDERAL PUBLIC ADMINISTRATION

Abstract
This paper proposes a model for Information Security Governance for the Federal Public Administration to be applied in any public agency. The general objective of this research is to propose the applicability, in relation to maturity levels, of the Information and Communications Security Governance model. The model presented aligns with the principles of Information Security, applicable laws and regulations, and with the good corporate governance of public entities. When the model is applied in an organization, it is possible to identify the maturity stage of Information Security Governance within the institution,

highlight areas for improvement, and compare with other institutions that apply the mentioned model. Regarding the methodology, this work consists of descriptive research that used standardized data collection techniques, in which the model was analyzed through respondents' answers to questions about the relevance of the concepts addressed in the model. Additionally, it is also a practical application that aimed to validate the construction of the mentioned model. The results include the possibility of assessing the organization's information security maturity, the evolution of maturity over time, and the ability to compare with other organizations that also apply the model.

Keywords: *information security governance; maturity model; framework; public administration.*

1 INTRODUÇÃO

Segundo Rosseti (2007), governança corporativa é o sistema pelo qual as sociedades são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

O objetivo central dos sistemas de governança corporativa não é intervir na autonomia das organizações, mas equilibrar a competitividade e a produtividade da empresa com uma gestão responsável e transparente. No escopo da Administração Pública, a governança se dá com a aplicação sistemática das leis e da autorregulação que buscam gerar uma cultura de transparência e uma gestão com a participação da sociedade nas decisões públicas.

Segundo o Banco Mundial (1992), a definição geral de governança é o exercício da autoridade, controle, administração e poder de governo. Mais precisamente, é a maneira pela qual o poder é exercido na administração dos recursos sociais e econômicos de um país tendo em vista o seu desenvolvimento e, ainda, as implicações na capacidade dos governos de planejar, formular e implementar políticas e cumprir funções. Os dados e informações utilizados nas organizações constituem um ativo de valor intangível e estratégico uma vez que, sem o manejo e o uso de tais informações, não há qualquer fluxo de entrega de produto, serviço ou resultado. Drucker (1993), afirma que o ponto central que diferencia as organizações atuais é o manejo e a utilização da informação em sua completude e dentro do espaço e tempo corretos.

Assim, as informações organizacionais estão sujeitas a diversas ameaças e riscos que podem corromper um ou mais dos três princípios básicos da Segurança da Informação – SI, a saber: confidencialidade, integridade e a disponibilidade que, uma vez comprometidos, resultam em prejuízo das informações.

Com a expansão e o aprimoramento de ferramentas computacionais, a maioria das informações organizacionais são produzidas e processadas em equipamentos de tecnologia em sua forma digital e transitam em rede de computadores. A norma ABNT NBR ISO/IEC 27002 (ABNTa, 2013), que é aplicável à APF, fornece as boas práticas para a Gestão da Segurança da Informação, com o objetivo de estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de SI de uma organização no espaço cibernético, incluindo a seleção, a implementação e o gerenciamento de controles, considerando os ambientes de risco na organização. Contudo, a norma ABNT NBR ISO/IEC 27032 (ABNTb, 2013) fornece diretrizes para princípios e atividades de SI ao traçar os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança tais como a segurança de redes, a segurança da Internet e a proteção das infraestruturas críticas de informação e ferramentas de defesa tecnológicas.

O Tribunal de Contas da União (TCU, 2016), no objeto de fiscalização, um levantamento, realizado nos exercícios de 2015/2016, em 376 organizações da Administração

Púbica Federal, coletou informações sobre a situação da Governança de Tecnologia da Informação na APF. O relatório indica que a Gestão Corporativa da SI foi objeto de apreensão em todos os levantamentos anteriores devido à baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis.

Os dados estão embasados nos controles e objetivos de controle extraídos da norma técnica ABNT NBR ISO/IEC 27002:2013, bem como nas normas e diretrizes estratégicas do Departamento de SI e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR) e do Conselho Nacional de Justiça.

Apesar de ser o principal instrumento direcionador da Gestão da SI, os dados mostram que 70% das organizações sob análise dispõem de uma política de SI formalmente instituída, 67% possuem um comitê de SI formalmente instituído, 53% contam com um gestor de SI e, ainda, apenas 52% possuem uma política de controle de acesso às informações formalmente constituída. Nesse contexto, o cenário apontado pelo TCU indica a necessidade da GovSI na APF. A segurança da informação (SI) e a boa governança de TI constituem um desafio dentro da Administração Pública Federal (TCU, 2016, p. 40).

A lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), tem o propósito garantir a proteção de todos os dados pessoais tratados e utilizados dentro das organizações públicas e privadas.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

No contexto, será abordado o modelo de GovSI, com embasamento no documento Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF (Guimarães, 2016).

Diante dos riscos associados ao tratamento de informações na APF, das leis e regulamentos aplicáveis à SI, das recomendações dos órgãos de controle para promover a boa governança dos recursos públicos e das transformações na prestação de serviços aos cidadãos, que demandam maior agilidade, conveniência e eficiência nos gastos públicos, é imprescindível adotar práticas e modelos que assegurem a maturidade e a efetividade na gestão de recursos e informações do Estado.

Esta pesquisa tem por objetivo geral propor a aplicabilidade, em relação aos níveis de maturidade, do modelo de Governança de Segurança da Informação e Comunicações proposto em Guimarães (2016).

2 REFERENCIAL TEÓRICO

Nicholls e Brown (2014), defendem que a GovSI apresenta impacto direto no gerenciamento de riscos das organizações. Rebollo (2015) empenhou-se em mostrar que a Governança da Segurança é considerada o método mais apropriado para obter o controle dos processos críticos organizacionais e, ainda, para garantir o alinhamento com a estratégia definida.

Guimarães (2016) esclareceu que a GovSI e a Comunicação constituem um conjunto de políticas e processos cujo foco é a redução de riscos, o que aumenta o valor de produtos ou serviços da organização para os usuários. O propósito do estudo é estruturar um arcabouço de GovSI para o Governo Federal que esteja em conformidade com as leis e normas pertinentes e, ainda, que seja compatível com a Estratégia da Segurança e Comunicação da Informação e Segurança Cibernética da APF.

Segundo (Carcary, 2016), as cinco principais funções da boa GovSI, a saber, o alinhamento estratégico, o valor entregue, o gerenciamento de recursos, o gerenciamento de desempenho e mais o gerenciamento de riscos. Os autores defendem que essas funções não são um fim nelas mesmas, mas servem para nortear as tomadas de decisão nas organizações e entregam valor para a sustentabilidade organizacional.

Assim observa-se que as informações e as tecnologias de comunicação são importantes para a sobrevivência de uma organização, sendo mandatório que as práticas voltadas ao uso correto e eficiente das informações, instituídas nos mais altos níveis estratégicos, sejam praticadas por todos de forma geral e orquestrada.

No quesito Governança, existem três processos basilares: avaliar, dirigir e monitorar, embasados pelo COBIT 5, quando aplicados à SI, tornam-se uma diretriz para a Governança direcionar todos os aspectos de proteção de informações corporativas para o cumprimento dos seus objetivos. As práticas de Governança da Segurança devem assegurar que as atividades e as diretrizes estratégicas sejam implementadas e, igualmente, que as atividades de monitoramento tenham como finalidade os controles introduzidos.

Outro ponto importante é o papel da GovSI no Gerenciamento de Riscos, o qual compreende o conjunto de atividades, estruturas e processos voltados para garantir que os riscos relacionados à SI sejam gerenciados e reduzidos a níveis aceitáveis para a manutenção e continuidade dos negócios da entidade.

2.1 Governança de Segurança da Informação

A norma ISO-IEC-27014/2013 (ISO, 2013) é a fonte de referência que fornece orientação sobre conceitos e princípios para a GovSI e pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a SI dentro da organização. É aplicável a todos os tipos e tamanhos de organizações. De acordo com a norma, são seis os princípios-chave (ISO, 2013): estabelecer a SI em toda a empresa, adotar uma abordagem baseada em riscos, estabelecer a direção de decisões de investimento, assegurar conformidade com os requisitos internos e externos, promover um ambiente positivo de segurança e analisar criticamente o desempenho em relação aos resultados de negócios.

Yaokumah e Brown (2014), tratam o conceito de GovSI como uma decisão a ser tomada pelo alto nível organizacional e alinhada ao gerenciamento de riscos.

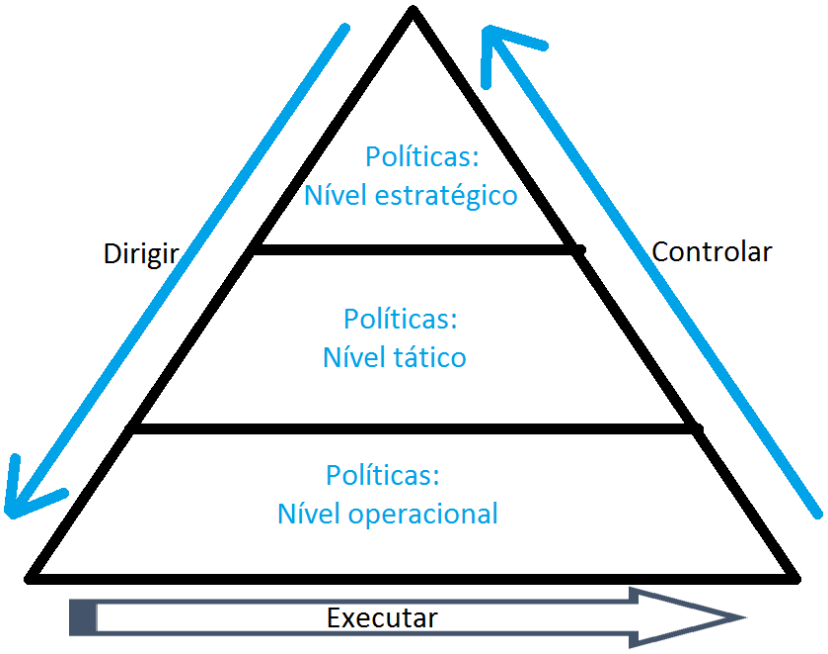
Com o intuito de mostrar a GovSI de forma mais objetiva e com foco nos critérios de SI alinhados às perspectivas organizacionais, os autores Carcary et alli. (2016) propuseram que a governança de SI e gestão (ISGM) concentra-se em determinar a capacidade da organização para supervisionar e controlar as ações e os processos necessários para proteger os sistemas de informação e comunicação.

Laksono e Supriyadi (2015) propõem a GovSI com base no *framework Control Objectives for Information and Related Technology*, na publicação de SI no guia COBIT 5 para SI, onde apontam que os objetivos de controle para informações e tecnologia relacionados no modelo em apreço é abrangente e especificam um conjunto de informações necessárias para atingir as metas de governança organizacionais. De acordo com Laksono e Supriyadi (2015, p. 18), "Implementação da governança de SI tem, basicamente, o propósito de apoiar a realização de objetivos e reduzir riscos organizacionais".

Von Solms, e Maninjwa (2016) abordam o conceito de GovSI centrado na arquitetura organizacional onde há um alinhamento da estrutura organizacional com a segurança requerida. Os autores propõem o tratamento da GovSI na mesma estrutura da governança corporativa e mostram que a existe a orquestração da reunião de pessoas, sistemas e tecnologias, ferramentas e políticas de gestão tendo como premissa básica a governança da Gestão de Riscos. A política abrangente de SI é exibida em forma de pirâmide, os três prismas

são: dirigir, controlar e executar, suas subdivisões abarcam os níveis estratégicos, tático e operacional (Figura 1).

Figura 1: Política Abrangente de Segurança da Informação



Fonte: Thomson, K. L (2011)

Antoniou (2017) mostra que a GovSI está alinhada com todas as outras áreas pertinentes da organização, enfatizando que não se pode dissociar requisitos de salvaguarda de informações dos processos de negócio. O autor mostra que o planejamento e a execução em conjunto de estratégias de SI e gestão de TI geram o compartilhamento e reutilização de recursos e, ainda, uma maior interação com as áreas finalísticas da organização.

William e Shawon (2018) tratam do conceito de Governança de SI voltada à gestão de riscos e controles internos da organização. Eles expõem a ideia do alinhamento com os requisitos de negócio e o nível de detalhes de implementação de controles e governança de riscos organizacionais que, por sua vez, encontram limitadores como recursos financeiros, cultura organizacional, fatores ambientais, dentre outros.

Nos conceitos tratados pelos autores, deduz-se que a GovSI está alinhada com a governança corporativa e está pautada no tripé da governança, a saber, avaliar, dirigir e monitorar, sempre com foco no gerenciamento de riscos de forma preventiva com vistas à perenidade de aumento de confiabilidade organizacional.

2.2 Modelo de Maturidade

Siqueira (2005) aponta para a maturidade em processos, uma abordagem disciplinada para identificação dos processos críticos e definição de ações de melhoria alinhadas com os objetivos estratégicos do negócio e consistentes com o estágio de maturidade de seus processos. O autor relata que o nível de maturidade é aplicado à maneira com que as organizações conduzem seus processos, de modo sistemático ou não.

Segundo Oliveira (2017), a maturidade organizacional é alcançada com ações conscientes e planejamento sistemático com o intuito de aperfeiçoar os diversos processos da

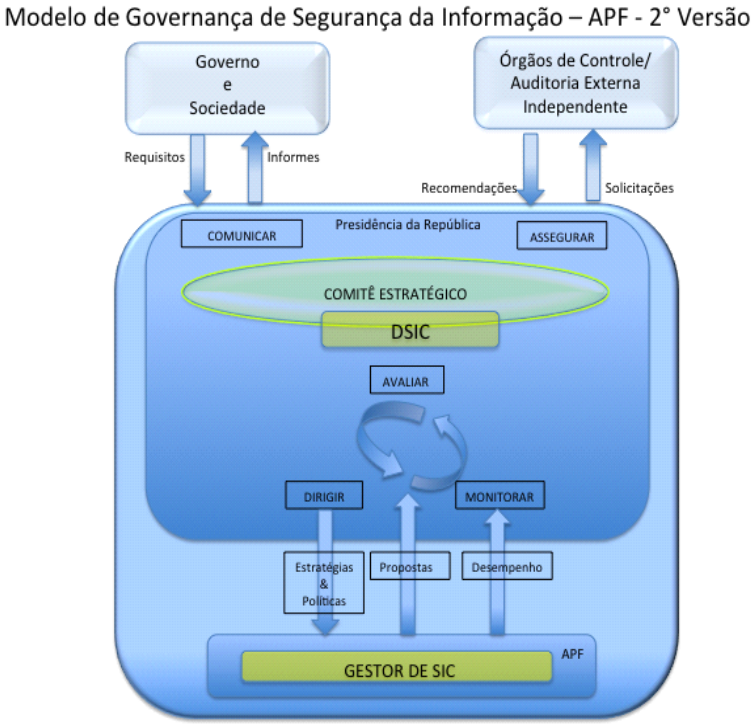
organização a fim de cumprir o proposto esperado. No contexto da TI existem modelos de maturidade para aplicação nas organizações, apresentados a seguir.

O CMMI (Modelo Integrado de Maturidade em Capacidade) desenvolvido pelo SEI (*Software Engineering Institute*) (CHRISSIS, 2010) procura estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas. O CMMI é um comprovado conjunto de práticas globais recomendadas que impulsiona o desempenho dos negócios por meio da criação e do benchmarking de recursos-chave. Este modelo possui duas representações: contínua ou por estágios, as quais permitem à organização utilizar diferentes caminhos para a melhoria de acordo com seu interesse.

No âmbito de SI, o *Cybersecurity Capability Maturity Model* - C2M2 (US Department of Energy, 2022) funciona como uma ferramenta muito flexível para uso dos proprietários e operadores em uma ou mais atividades tais como: Identificar uma abordagem progressiva, funcionar como referência, priorizar ações e investimentos, medir e demonstrar o progresso ao longo do tempo em direção a objetivos específicos da organização de forma consistente, compartilhar conhecimento de Segurança Cibernética entre as organizações; e possibilitar a definição de quais recursos e ativos devem ser priorizados no âmbito da Segurança Cibernética.

A estrutura de aplicação do presente modelo tem como base o modelo de SI proposto por Guimarães (2016), que busca demostrar a estrutura básica da Governança da Segurança da Informação na Administração Pública Federal (Figura 2).

Figura 2: Versão final do Modelo de Governança de Segurança da Informação para a APF



Fonte: Guimarães (2016)

Os principais elementos transitados pelos processos e os atores envolvidos na sistemática de governança são (Guimarães, 2016, p. 95-96):

- Requisitos: demandas, questionamentos, solicitações do Governo ou da sociedade sobre SI e Comunicação.

- Informes: respostas, esclarecimentos, informativos sobre SI e Comunicação na APF ou sobre demanda específica.
- Solicitações: pedidos de informações, análise de proposições, resultados de auditorias realizadas.
- Recomendações: sugestões de melhorias sobre SI e Comunicação na APF ou pareceres/análise sobre proposições.
- Estratégias & Políticas: orientações, direcionamentos, sobre SI e Comunicação para a APF.
- Propostas: sugestões de melhorias ou alterações em estratégias, políticas e orientações dos gestores de SI e Comunicação dos órgãos e entidades da APF.
- Desempenho: informe sobre os indicadores de metas estabelecidas sobre SI e Comunicação.

Desse modo, explicita a limitação de pesquisa e ainda a sugestão para trabalhos futuros (Guimarães, 2016, p. 101). A pesquisa teve como limitações o fato de apresentar um modelo conceitual que não foi implementado para teste de sua viabilidade e de sua efetividade.

3 METODOLOGIA

Lakatos (1991), afirma que a pesquisa bibliográfica requer um conjunto ordenado de procedimentos para a busca de soluções, focado no objeto de estudo e que, por isso, não pode ser aleatório, mas deve ser estruturado e organizado com objetivo de validar o objeto de estudo e ser fonte de exploração ou contestações futuras. A autora classifica as diversas formas de pesquisa científica quanto à área da ciência, à natureza, aos objetivos, ao procedimento e à forma de abordagem do problema.

A pesquisa possui um objetivo descritivo acerca do tema proposto pois explora conceitos e esclarece fatos e implicações que mostram o problema da GovSI na APF, e inclui a aplicação do modelo desenvolvido em uma instituição vinculada à APF.

O procedimento adotado para tratar o tema proposto é a pesquisa bibliográfica envolvendo o levantamento de referências teóricas já validadas e publicadas em meios escritos e eletrônicos com o objetivo de adquirir conhecimento prévio sobre o assunto e, assim, abordar o modelo proposto de forma mais focada e pertinente além de elaborar a proposta do modelo de maturidade em GovSi. Aborda, ainda, uma pesquisa com gestores de SI para a validação do modelo e finalmente aplica o modelo em um órgão da APF.

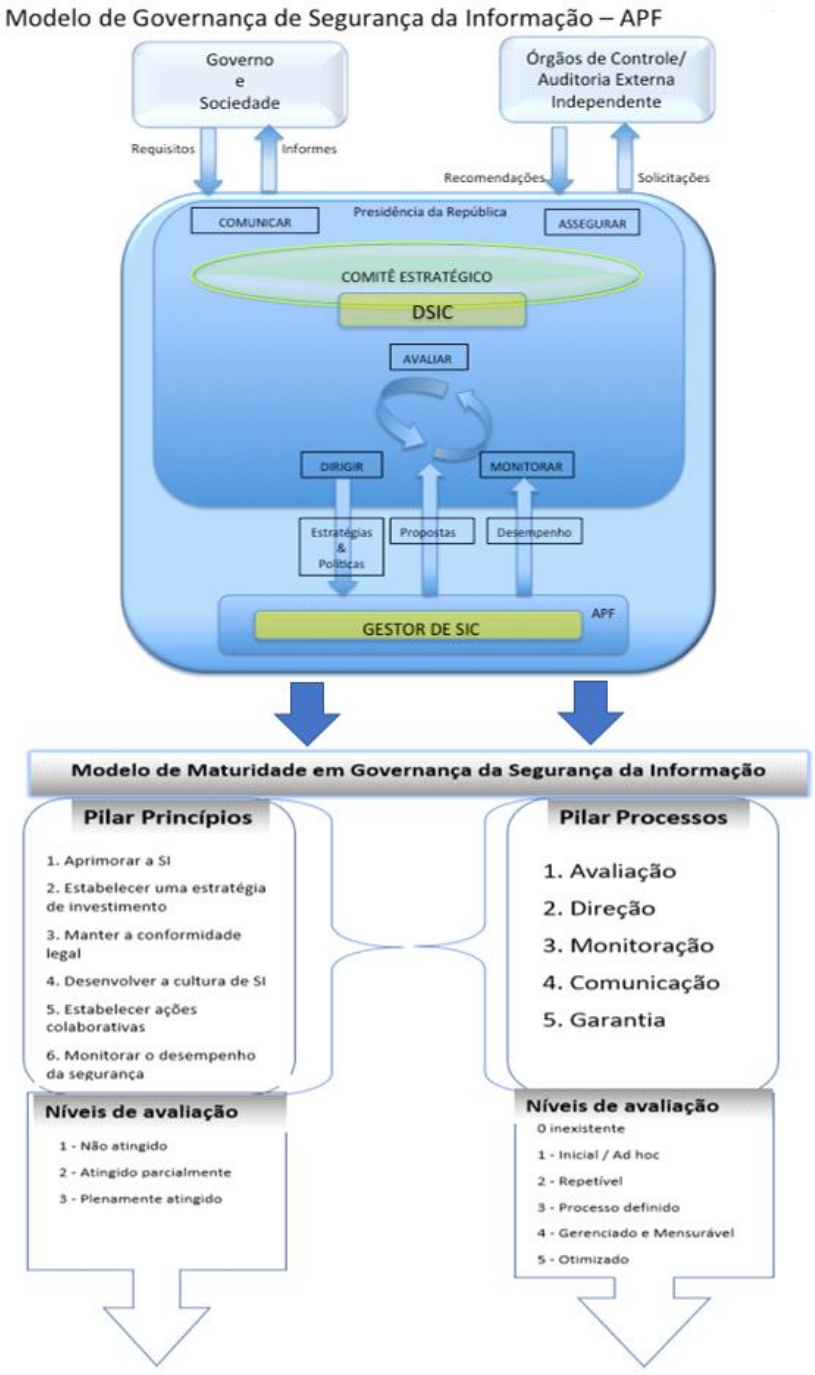
4 PROPOSTA DE MODELO

O modelo de maturidade é estruturado em dois pilares fundamentais: os princípios e os processos, que buscam minimizar os riscos na APF, como maior agilidade na tomada de decisões frentes aos riscos da informação, a redução de custos, a efetividade dos investimentos em SI e a conformidade legal.

O presente apresenta a estrutura composta por dois pilares principais: os **princípios** e os **processos**. Os princípios fornecem as diretrizes estratégicas fundamentais, como aprimorar a segurança da informação, estabelecer estratégias de investimento, manter a conformidade legal, desenvolver uma cultura de segurança, promover ações colaborativas e monitorar o desempenho. Já os processos são estruturados para garantir a implementação efetiva e o acompanhamento dessas diretrizes, com atividades como avaliação contínua, direcionamento estratégico, monitoração de resultados, comunicação efetiva e garantia da conformidade. Essa combinação visa integrar a segurança da informação de forma holística, alinhando-a aos objetivos organizacionais e às exigências legais, enquanto promove a maturidade e a eficiência na gestão de recursos e informações na Administração Pública Federal.

A Figura 3 mostra graficamente a aplicabilidade do modelo proposto a partir do modelo genérico apresentado por Guimarães (2016).

Figura 3: Derivação do modelo de maturidade em Segurança da Informação para a APF



Fonte: os autores

Figura 4: Derivação do modelo de maturidade em Segurança da Informação para a APF.

Fonte: os autores

4.1 Pilar Princípios

Princípio 1: Aprimorar a Segurança da Informação

O objetivo deste princípio é a coordenação da SI na sua infraestrutura, atribuindo responsabilidades específicas para cada atividade desempenhada pelos agentes do Estado e, ainda, envolver a sociedade como parte ativa e atuante que contribui diretamente para que o princípio seja alcançado.

Princípio 2: Estabelecer uma estratégia de investimento

A priorização e o planejamento dos investimentos tanto nas ações atuais quanto nas futuras com a colaboração entre entidades públicas e privadas, para que o investimento financeiro em SI seja razoável, efetivo e transparente, com retorno para a sociedade.

Princípio 3: Manter a conformidade legal

As instituições devem atentar para as leis e regulamentos pertinentes à sua área de atuação, as normas de SI e, ainda, o pleno alinhamento com requisitos regulatórios internos e externos.

A GovSI deve assegurar que a política de SI e as ações de gestão de SI de cada instituição da APF cumpram o estabelecido em leis e normas nacionais e, mais, que atendam a requisitos contratuais internos e externos.

Princípio 4: Desenvolver a cultura de SI

Este princípio estimula a educação e conscientização em SI, promovendo mudanças comportamentais tanto de pessoas quanto das instituições, de forma a obter uma postura humana responsável e consciente e, ainda, elevar o grau de maturidade das instituições, levando em consideração que o comportamento humano é essencial para atingir os níveis de segurança desejados.

Princípio 5: Estabelecer ações colaborativas

Este princípio considera que a SI jamais pode estar isolada em um órgão ou processo específico. Assim, deve ser constantemente promovida a articulação e o desenvolvimento de parcerias entre as instituições públicas e privadas, visando o desenvolvimento dos agentes do Estado, para a adoção de boas práticas, novas soluções tecnológicas e de estímulo ao desenvolvimento de serviços com alto grau de confiança.

Princípio 6: Monitorar o desempenho da segurança

Neste princípio é promovida a busca da garantia de funcionamento da SI em plena conformidade com os parâmetros estabelecidos. O monitoramento deve ser holístico, contínuo, procurando identificar o desempenho da SI desde o estabelecimento dos parâmetros pertinentes até a entrega efetiva de valor para a sociedade.

Para avaliar o Pilar Princípios, foi utilizada uma escala que possui três níveis, 1 – Não atingido, 2 - Atingido parcialmente e 3 - Plenamente atingido. Os critérios de avaliação são específicos para cada princípio e são evolutivos, ou seja, para atingir um nível é necessário cumprir o anterior, em observação ao questionado.

Princípio 1: Aprimorar a SI.

- Nível 1 – Não atingido: Neste patamar não existe o mapeamento da infraestrutura crítica e não existem responsabilidades definidas para processos de SI. Os incidentes são respondidos à medida que acontecem.
- Nível 2 - Atingido parcialmente: A organização documenta e protege suas informações críticas, atribui papéis e responsabilidades para a Gestão de Ativos Informacionais.
- Nível 3 - Plenamente atingido: A organização adota processos de redundância de proteção à infraestrutura crítica, estabelece treinamentos constantes dos colaboradores e dos usuários e a sociedade já possui interesse em proteger as informações usadas. Existe, ainda, um monitoramento contínuo de eventos que podem comprometer a SI.

Princípio 2: Estabelecer uma estratégia de investimento

- Nível 1 – Não atingido: Não existe qualquer investimento em SI, os recursos financeiros são categorizados como gastos em respostas reativas a incidentes.
- Nível 2 - Atingido parcialmente: Existe o planejamento e o investimento de ativos organizacionais em equipamentos e tecnologias de SI, porém eles são provenientes do aprendizado com incidentes anteriores. Não há colaboração com outras entidades e nem compartilhamento de recursos, além de não serem prestadas contas dos investimentos realizados para a sociedade.
- Nível 3 - Plenamente atingido: Planeja e prioriza os investimentos em SI, agindo de modo proativo e de maneira sustentável. Inclui a colaboração contínua com entidades públicas e privadas, o compartilhando de recursos e informações e, ainda, muita confiabilidade da sociedade nas ações da organização.

Princípio 3: Manter a conformidade legal

- Nível 1 – Não atingido: Desconhece qualquer norma que envolva a SI e constantemente reage em resposta à obrigatoriedade de cumprimento da legislação.
- Nível 2 - Atingido parcialmente: Conhece e aplica as normas e leis pertinentes à SI em alinhamento com a estratégia organizacional, porém não possui qualquer controle interno ou externo, ou, se o possui, não atua na fiscalização do cumprimento dos requisitos legais que dizem respeito à SI. A organização possui uma política de SI que não é revisada constantemente e que depende de atualizações reativas.
- Nível 3 - Plenamente atingido: Existe o mapeamento das leis e normas pertinentes à área de atuação, o cumprimento dessas normas é irrestrito e, ainda, suas normas internas englobam plenamente e de forma adequada as leis pertinentes. Algumas unidades organizacionais cuidam para o efetivo cumprimento dessas leis e normas concernentes que alinham SI, área de negócio, requisitos legais e contratuais. Portanto, existe um atuante controle interno e externo

e a organização possui uma política de SI atualizada e divulgada às partes interessadas pertinentes.

Princípio 4: Desenvolver a cultura de SI

- Nível 1 – Não atingido: A organização não promove treinamentos nem cuida da conscientização dos colaboradores no quesito SI. O comportamento dos colaboradores é intuitivo e não existe uma direção clara a ser seguida.
- Nível 2 - Atingido parcialmente: A organização mostra evidências de reconhecimento da necessidade de abordagem do princípio de SI e, deste modo, a conscientização da SI é incorporada aos processos organizacionais. Os treinamentos são direcionados apenas aos colaboradores-chave.
- Nível 3 - Plenamente atingido: A organização faz constantes treinamentos dirigidos a diversos públicos de colaboradores, exige um comportamento responsável e transparente bem como os papéis e responsabilidades em SI são definidos, atribuídos e implementados de forma proativa. Consequentemente, a cultura de SI torna-se um objetivo estratégico da organização que, então, passa a possuir um modelo de Gestão de Risco de SI adequado à sua estratégia.

Princípio 5: Estabelecer ações colaborativas

- Nível 1 – Não atingido: Não possui processos que atentam para a SI.
- Nível 2 - Atingido parcialmente: A SI é realizada ao lado dos processos organizacionais, porém ela não possui qualquer interlocução com entidades especializadas e a fonte de requisitos da SI tem sempre origem nos objetivos organizacionais e reativos aos incidentes. As atividades de salvaguarda das informações se limitam ao contexto organizacional.
- Nível 3 - Plenamente atingido: Integra a SI em todos os processos organizacionais e promove uma constante articulação com outras instituições públicas e privadas. Possui canais eficientes de comunicação com órgãos especializados em incidentes de SI e Controle de Riscos e, também, ações antecipadas a eventos que possam comprometer as informações organizacionais.

Princípio 6: Monitorar o desempenho da segurança

- Nível 1 – Não atingido: Por não haver aplicação sistemática da SI, não há monitoramento.
- Nível 2 - Atingido parcialmente: A organização monitora apenas o desempenho da SI que está ligada a ativos estratégicos críticos, aceitando pontos de falha ou desempenho abaixo do que foi acordado. Desta forma, a organização é proativa quando faz a salvaguarda de ativos críticos e de alto valor financeiro e é reativa em relação aos ativos que são críticos para a continuidade do negócio.
- Nível 3 - Plenamente atingido: A organização mostra a garantia de funcionamento da SI em plena conformidade com os parâmetros estabelecidos. Há o completo mapeamento de eventos associados aos incidentes de SI, assim como existe pro atividade para a tomada de decisão frente aos riscos à salvaguarda de ativos de informação.

4.2 Pilar Processos

Segundo Guimarães (2016), os responsáveis pela GovSI devem garantir que o responsável pela gestão de SI de suas instituições implemente a estratégia definida e as ações necessárias de SI que suportem as ações e políticas públicas. Assim sendo, os processos a respeito de direção, monitoração, comunicação e garantia, são abordados pela seguinte ótica:

- Processo Avaliação: Processo necessário para a visão de progresso da implantação do modelo, com uma avaliação sistemática, ponderando os recursos alocados e os resultados alcançados. Por meio dessa avaliação, que deve ser contínua, a estratégia redefine planos e metas para toda a SI dentro da organização, possibilita ainda comparar resultados de avaliações posteriores e visualizar o progresso das ações implementadas.
- Processo Direção: Este processo busca o direcionamento dos objetivos e estratégias de SI que devem ser implementados, incluindo, a gestão de recursos, planos de gestão de riscos, priorização de atividades e políticas e aceitação de riscos. Para viabilizar este processo, os responsáveis pela Governança de SI devem assegurar a implementação da estratégia nas organizações em que atuam, o alinhamento da SI com objetivos da organização e, ainda, promover a absorção dos aspectos de SI na cultura organizacional.
- Processo Monitoração: Este processo visa validar a geração de valor com a implementação dos objetivos estratégicos de SI. Para realizar este processo, a GovSI deve avaliar a eficácia da SI e a sua conformidade com os requisitos internos e externos, avaliar as alterações de cenários e os riscos às informações. Para viabilizar este processo, é necessário que as auditorias sejam realizadas pelos órgãos de controle e que sejam estabelecidas métricas de desempenho de Gestão de SI.
- Processo Comunicação: Aqui são avaliadas formas, tempestividade e efetividade dos canais de comunicação entre todos os atores envolvidos na SI. Na execução deste processo é necessária a análise da clareza e completude do processo de transparência que deve ser mantida entre as diversas partes interessadas.
- Processo de Garantia: Este processo consiste no relacionamento entre os órgãos de controle e auditoria e a organização, observando-se o grau de manutenção dos níveis de SI conforme foi desenhado na estratégia e, ainda, o uso dos relatórios e apontamentos dos controles como retroalimentação da estratégia.

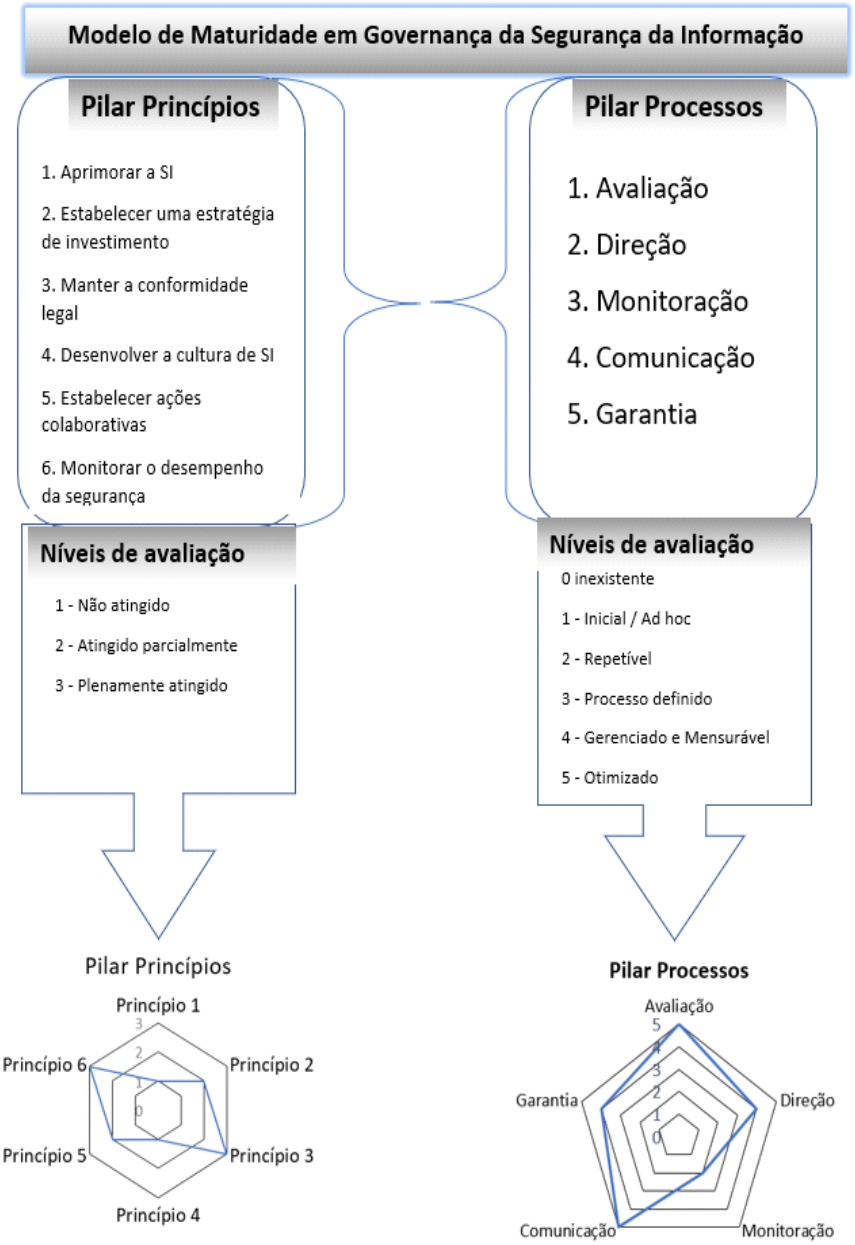
Para a avaliação dos processos do modelo proposto serão usados os níveis de maturidade do CobiT 4.1. A escolha do modelo de maturidade do CobiT 4.1 justifica-se pelo fato de essa versão ser orientada exclusivamente em processos, com a avaliação da sua maturidade, e que esteja plenamente alinhado com a GovSI. Um modelo de processos incentiva a determinação de proprietários dos processos, o que possibilita a definição de responsabilidades. Assim, os níveis de maturidade que serão aplicados no modelo são:

- Nível 0 - Inexistente – A organização desconhece qualquer processo de SI. Não há conhecimento de qualquer questão a ser trabalhada.
- Nível 1 - Inicial / Ad hoc – Existem evidências do reconhecimento da existência de questões que precisam ser abordadas. Mesmo assim, não existe processo padronizado pois ainda há enfoques Ad Hoc que tendem a ser aplicados isoladamente nos processos de SI. O gerenciamento é desorganizado.
- Nível 2 - Repetível, porém intuitivo – Os processos evoluíram para uma padronização na execução dos processos, porém não há um treinamento formal ou comunicação dos procedimentos padronizados, sendo que a responsabilidade é deixada com o indivíduo. Existe muita confiança no conhecimento concentrado em colaboradores específicos, podendo ocorrer falhas.
- Nível 3 - Processo definido – Há uma padronização, documentação e treinamentos nos processos. Tem-se a formalização de práticas, porém não existe sofisticação nos processos. Ainda existem dificuldades em corrigir desvios.
- Nível 4 - Gerenciado e Mensurável – Neste nível existe o monitoramento e adesão dos procedimentos de SI e é possível detectar falhas e corrigir o curso de ações necessárias. Os processos estão em um constante aprimoramento e fornecem boas práticas. A automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.

- Nível 5 - Otimizado – Aqui há um refinamento constante e uso de boas práticas com base no resultado de um aprimoramento contínuo e a modelagem da maturidade, como em outras organizações. A SI é utilizada como um caminho integrado para assegurar a constante entrega de valor com o uso de ferramentas corretas e decisões proativas.

A Figura 5 representa graficamente o desdobramento dos pilares, seus níveis de avaliação de maturidade e expõe um "gráfico de em rede", onde mostra que quanto maior a área de exposição alcançada no gráfico, maior será a maturidade da organização avaliada, dentro do respectivo pilar.

Figura 5 – Proposta do Modelo de Maturidade em GovSI na Administração Pública Federal.



Fonte: os autores

5 RESULTADOS

A pesquisa relacionou 16 questões, divulgada na rede social LinkedIn, informando o resumo da pesquisa e atraindo a atenção para a pesquisa direcionada aos profissionais interessados, não obrigatórias, e contou com 43 respondentes.

O perfil dos pesquisados foram gestores e profissionais da governança corporativa da Administração pública federal.

A primeira pergunta busca traçar o setor de atuação dos respondentes, procurando saber em qual grupo de instituição os respondentes estão concentrados. Dentre os participantes, a grande maioria concentrou-se no grupo de atuantes em instituições públicas.

A segunda questão tem o objetivo de elucidar a necessidade de a organização adotar um modelo de referência para guiar a GovSI. Todos os respondentes julgaram que sim.

A terceira questão aborda a pertinência da GovSI ser embasada nos processos de avaliação, direção e monitoramento. Nesta questão 97,67% dos respondentes julgaram ser necessária a adoção abordada.

A quarta questão investiga a pertinência da abordagem do princípio “aprimorar a SI”. Este princípio procura a coordenação da SI nas infraestruturas críticas, a saber, servidores e equipamentos tecnológicos, links de comunicação, sites e aplicações da web, dentre outros, atribuindo responsabilidades específicas para cada atividade desempenhada pelos agentes do Estado. E envolve, ainda, a sociedade como parte ativa e atuante que contribui diretamente para o alcance do princípio ao procurar uma contínua melhoria da SI no âmbito organizacional.

A quinta pergunta questiona a opinião dos respondentes sobre a relevância do princípio “Estabelecer uma estratégia de investimentos em SI”. Este princípio trata da priorização e planejamento dos investimentos, tanto nas ações atuais quanto nas futuras, com a colaboração entre entidades públicas e privadas para que o investimento financeiro em SI seja razoável, efetivo e transparente, com retorno para a sociedade. Como apresentado, 97,22% dos respondentes julgam muito útil a abordagem do referido princípio.

A sexta questão aponta para questões legais e normativas quando questiona a importância de se discutir o princípio da conformidade legal com as abordagens de SI. O princípio em causa determina que as instituições devem estar atentas às leis e regulamentos pertinentes à sua área de atuação, às normas de SI e, ainda, ao pleno alinhamento com os requisitos regulatórios internos e externos.

A sétima questão procura saber a opinião dos respondentes sobre a utilidade da abordagem do princípio “Desenvolver a cultura da SI”. Este princípio visa estimular a educação e a conscientização em SI ao propor mudanças comportamentais, tanto de pessoas quanto das instituições, com o intuito de obter uma postura humana responsável e consciente. Mais ainda, propõe elevar o grau de maturidade das instituições, levando em consideração que o comportamento humano é essencial para o atingimento dos níveis de segurança desejados.

A oitava pergunta tem o propósito de validar o princípio “Estabelecer ações colaborativas em SI”, o qual considera que a SI nunca pode ser isolada em um órgão ou processo específico. Consequentemente, devem ser constantemente promovidos a articulação e o desenvolvimento de parcerias entre as instituições públicas e privadas visando o desenvolvimento dos agentes do Estado para a adoção de boas práticas, novas soluções tecnológicas e de estímulo ao desenvolvimento de serviços com alto grau de confiança. Assim, 47 respondentes, ou 89,10%, julgaram muito útil a abordagem desse princípio dentro do modelo.

A nona questão, indaga sobre o princípio “Monitorar o desempenho da SI”. O princípio em causa procura mostrar e garantir o funcionamento da SI em plena conformidade com os parâmetros estabelecidos. O monitoramento deve ser holístico, contínuo, procurando

identificar o desempenho da SI desde o estabelecimento dos parâmetros pertinentes até a entrega efetiva de valor para a sociedade. Os resultados indicam que dos 37 respondentes, 94,59% confirmam ser muito útil a abordagem desse princípio listado no modelo proposto.

A décima questão: "Para sugerir um princípio, utilize o campo abaixo", solicita a opinião do respondente, de forma aberta e textual, para estimular sua opinião sobre a mencionada questão e, ainda, a possibilidade de o respondente propor algum princípio que julgar pertinente, sendo que, das 16 respostas, destacam-se as sugestões de princípios mais pertinentes: (i) Integridade (assegurar que toda informação corporativa não seja alterada); (ii) Segurança de garantia de rastreio de fontes de dados; (iii) Desenvolvimento da biometria para ajudar na SI; (iv) Confidencialidade, integridade, disponibilidade (CID) da SI; (v) Agilidade no atendimento das demandas solicitadas pelos colaboradores na área da SI; (vi) Responsabilização; (vii) Sigilo documental; (viii) Confiança e celeridade em cooperações.

Quadro 1: Resultado da pesquisa no pilar princípios

Princípio	Utilidade de abordagem dos princípios (%)		
	Muito útil	Indiferente	Nada útil
Aprimorar a SI	97,30	2,70	0,00
Estabelecer uma estratégia de investimento	97,22	2,78	0,00
Manter a conformidade legal	97,30	2,70	0,00
Desenvolver a cultura de SI	97,22	2,78	0,00
Estabelecer ações colaborativas	89,19	10,81	0,00
Monitorar o desempenho da SI	94,59	5,41	0,00

Fonte: Dados da pesquisa (2024)

No Pilar Processos, a pesquisa buscou abordar a concordância dos processos apresentados dentro do modelo proposto, onde cada processo pode ser julgado como pertinente, ou não, ao modelo proposto, de acordo com a opinião do respondente.

A décima primeira questão procura saber a opinião dos respondentes acerca da pertinência do processo "Avaliação" com o objetivo de mensurar o alcance dos objetivos de SI. Igualmente, é a base para a correção de desvios e aumento da visibilidade dos gargalos e imprevisibilidades no alinhamento estratégico da SI com os requisitos de negócio, no contexto da GovSI. O gráfico indica que 83,33% dos respondentes julgam muito útil a abordagem do processo de avaliação dentro do modelo proposto.

A décima segunda questão aponta para a pertinência do processo de "Direção". Este princípio visa o direcionamento dos objetivos e estratégias de SI que precisam ser implementados, incluindo a gestão de recursos, planos de gestão de riscos, priorização de atividades e políticas, e a aceitação de riscos, presentes no modelo sob análise. Dos 36 respondentes, 91,67%, reconhecem ser muito útil a abordagem desse processo dentro do modelo.

A décima terceira questão aborda a pertinência do processo de "Monitoração". Este princípio visa validar a geração de valor com a implementação dos objetivos estratégicos de SI. Para realizar este processo, a Governança de SI deve avaliar a eficácia da SI e a sua conformidade com os requisitos internos e externos. As respostam indicam que dos 36 respondentes, 94,44%, julgam muito útil a utilização do referido processo no modelo.

A décima quarta questão procura saber a opinião acerca do processo de "Comunicação", o qual avalia a tempestividade e a efetividade dos canais de comunicação com todos os atores envolvidos na SI. Para executar este processo, é procedida a análise da clareza e completude do processo de transparência que deve ser mantido com as diversas partes interessadas e sua adesão ao modelo proposto. Os resultados mostram que dos 36

respondentes, 97,22%, julgam muito útil a inclusão do processo no modelo de avaliação sob análise.

A décima quinta questão inclui a opinião acerca do processo de "Garantia", cujo objetivo é manter o relacionamento dos órgãos de controle externo e de auditoria interna com a organização. Assim, foram obtidas 36 respostas e 80,56% dos respondentes julgaram muito útil a abordagem do princípio questionado.

A décima sexta questão: "Para sugerir um processo, utilize o campo abaixo", teve o intuito de buscar a colaboração e sugestão dos respondentes no pilar processos. Foram obtidas 13 respostas, com destaque para as seguintes opiniões: (i) Controle; (ii) Monitoramento de crises; (iii) Contingência; (iv) Manter regras de segurança atualizadas e divulgá-las; (v) Comunicação célere; (vi) Aculturamento. Os dados obtidos da análise da pesquisa são satisfatórios e fornecem embasamento para aplicação do referido modelo.

Quadro 2: Resultado da pesquisa no pilar processos

Processos	Utilidade de abordagem dos processos (%)		
	Muito útil	Indiferente	Nada útil
Avaliação	83,33	16,67	0,00
Direção	91,67	8,33	0,00
Monitoração	94,44	5,56	0,00
Comunicação	97,22	2,78	0,00
Garantia	80,56	16,67	2,78

Fonte: Dados da pesquisa (2024)

Para proceder a aplicação do modelo proposto, foram escolhidas as duas instituições pertinentes, ligadas à APF, sendo identificados gestores com conhecimento especializado na área de SI e com atuação no âmbito de gestão de informações sensíveis, os quais foram alocados no órgão em cargos estratégicos. O convite aos gestores escolhidos foi aceito, sendo então agendada uma entrevista na qual o modelo foi apresentado e explicados os quesitos a serem abordados. A aplicação do modelo foi feita em uma Organização Social, vinculada à Administração Pública Federal do Poder Executivo Federal com atuação em todo território nacional. De acordo com os questionamentos apresentados, foram obtidos os seguintes dados, apresentados na sequência.

5.1 Avaliação do Pilar Princípios

Princípio 1: Aprimorar a SI

A finalidade deste princípio é a coordenação da SI na sua infraestrutura crítica, atribuindo responsabilidades específicas para cada atividade desempenhada pelos agentes do Estado e, ainda, o envolvimento da sociedade como parte ativa e atuante que contribui diretamente para o alcance do princípio.

Respondente (R): A organização cuida, apenas, da infraestrutura crítica e atribui papéis e responsabilidades aos colaboradores que têm a guarda dessa infraestrutura.

Deste modo, a organização encontra-se no nível 2, atingido parcialmente, no qual suas informações críticas estão protegidas. São atribuídos papéis e responsabilidades para a gestão de ativos informacionais.

Princípio 2: Estabelecer uma Estratégia de Investimento

O segundo princípio trata da priorização e planejamento dos investimentos nas ações atuais e futuras, com a colaboração entre entidades públicas e privadas, para que o

investimento financeiro em SI seja razoável, efetivo e transparente e apresente retorno para a sociedade.
R: A organização aborda a SI como uma despesa e, assim, aloca os recursos para reparar o dano advindo de algum incidente.

Neste contexto, a organização encontra-se no nível 1, não atingido, no qual não existe qualquer investimento em SI e os recursos financeiros são categorizados como despesas em respostas reativas a incidentes.

Princípio 3: Manter a Conformidade Legal

O terceiro princípio visa disseminar a noção de que as instituições devem atentar para as leis e regulamentos pertinentes à sua área de atuação, às normas de SI e, ainda, ao pleno alinhamento com requisitos regulatórios internos e externos.
R: A organização conhece e aplica as normas pertinentes, e por se tratar de entidade pública, encontra-se dentro de todo aparato legal e normativo, embora não possua controle externo e interno nos requisitos de SI. Todavia, a organização possui uma política de SI.

Deste modo, a organização encontra-se no nível 2, atingido parcialmente, no qual as normas e leis pertinentes à SI são conhecidas e aplicadas em alinhamento com a estratégia organizacional. Todavia, o controle externo não atua na fiscalização do cumprimento dos requisitos legais que dizem respeito à SI. É importante notar que, embora a organização possua uma política de SI, ela não é constantemente revisada e, assim, depende de atualizações reativas.

Princípio 4: Desenvolver a Cultura de SI

Este princípio procura estimular a educação e a conscientização em SI, promovendo mudanças comportamentais tanto de pessoas quanto das instituições, de forma a obter uma postura humana responsável e consciente e, igualmente, elevar o grau de maturidade das instituições levando em consideração que o comportamento humano é essencial para atingir os níveis de segurança desejados.
R: A organização utiliza vários canais de comunicação para a conscientização da SI, tais como palestras, panfletos, cartazes, entre outros. No entanto, o treinamento e a educação formal são dirigidos apenas aos ocupantes de cargos de alta gestão.

Em vista disso, a organização encontra-se no nível 2, atingido parcialmente, onde há evidências de reconhecimento da necessidade de abordagem do princípio em causa e, por consequência, a conscientização da SI é incorporada aos processos organizacionais. Os treinamentos são direcionados apenas aos colaboradores-chave.

Princípio 5: Estabelecer Ações Colaborativas

O princípio 5 aborda a noção de que a SI jamais pode estar separada em um órgão ou processo específico e, por isso, a articulação e o desenvolvimento de parcerias entre as instituições públicas e privadas deve ser constantemente promovida.
R: A SI é incorporada à estrutura e aos processos da organização. Existe a preocupação de manipulação da informação e o seu devido tratamento frente à segurança, porém não existe articulação com entidades especializadas externas para a salvaguarda de ativos. Os objetivos de SI são frequentemente oriundos de incidentes.

A organização está no nível 2, atingido parcialmente, no qual a SI é realizada junto aos processos organizacionais, mas, como não possui qualquer interlocução com entidades especializadas, a fonte de requisitos de SI é sempre oriunda dos objetivos organizacionais e reativos aos incidentes. As atividades de salvaguarda das informações se limitam ao contexto organizacional.

Princípio 6: Monitorar o Desempenho da Segurança

Este princípio verifica se a SI atende aos parâmetros estabelecidos por meio de uma monitoração contínua e holística. Cuida em manter um nível adequado de desempenho do nível da SI acordado.

R: Apenas são monitorados os ativos de informação estrategicamente críticos e dentro do escopo legal pois, na condição de uma entidade governamental ela deve obedecer às leis pertinentes e sempre age reativamente.

Deste modo a organização encontra-se no nível 2, atingido parcialmente, no qual a organização monitora apenas o desempenho da SI ligado a ativos estratégicos críticos, aceitando, portanto, pontos de falha ou desempenho abaixo do que foi acordado.

Conforme os dados do Quadro 3, nenhum processo encontra-se no nível 3, o nível máximo de avaliação, ou seja, Plenamente Atingido. Apenas o princípio 2, ou seja, "Estabelecer uma Estratégia de Investimento", encontra-se no nível 1 de maturidade, não atingido.

Quadro 3: Avaliação no Pilar Princípios pelo entrevistado

Princípios	Níveis de Avaliação		
	1– Não atingido	2- Atingido parcialmente	3- Plenamente atingido
Princípio 1: Aprimorar a SI		X	
Princípio 2: Estabelecer uma estratégia de investimento	X		
Princípio 3: Manter a conformidade legal		X	
Princípio 4: Desenvolver a cultura de SI		X	
Princípio 5: Estabelecer ações colaborativas		X	
Princípio 6: Monitorar o desempenho SI		X	

Fonte: Dados da pesquisa (2024)

5.2 Avaliação do Pilar Processos

Cada processo é avaliado em uma escala de seis níveis, de 0 a 5, progressivamente, de forma evolutiva. Seguem os dados da aplicação do modelo:

- Processo Avaliação: processo necessário para a visão de progresso da implantação do modelo com uma avaliação sistemática, ponderando os recursos alocados e os resultados alcançados.

  R: Os processos de SI relacionados ao cumprimento das normas e leis são avaliados bem como a manutenção de sistemas críticos. Todavia, os processos ainda são dependentes do conhecimento de servidores com a pertinente expertise.

  A organização encontra-se no nível 2, repetível, no qual os processos evoluíram para a padronização na execução dos processos, porém não há um treinamento formal ou uma comunicação dos procedimentos padronizados. Ainda mais, a responsabilidade é deixada com o indivíduo, pois a confiança é depositada no conhecimento concentrado em colaboradores específicos, o que pode ocasionar falhas.

- Processo Direção: o objetivo deste processo é o direcionamento dos objetivos e estratégias da SI que precisam ser implementados, o que inclui a gestão de recursos, planos de gestão de riscos, priorização de atividades e políticas, e aceitação de riscos.
  R: O direcionamento serve para o cumprimento das leis e manutenção dos ativos críticos. A gestão dos recursos, as atividades e a visão com relação aos riscos são muito dependentes do conhecimento de algumas pessoas.
  A organização encontra-se no nível 2, repetível, no qual os processos evoluíram para uma padronização na sua execução. A confiança está depositada no conhecimento concentrado em colaboradores específicos, podendo ocorrer falhas.
- Processo Monitoração: O objetivo deste processo é validar a geração de valor com a implementação dos objetivos estratégicos da SI, no qual a GovSI deve avaliar a eficácia da SI e a sua conformidade com os requisitos internos e externos e, ainda, avaliar as alterações de cenários e os riscos às informações.
  R: A organização não realiza um monitoramento sistemático da GovSI, não existem métricas claras de cumprimento de requisitos ou objetivos a serem alcançados. Frequentemente a organização age de forma reativa aos incidentes ocorridos na operação de sistemas e aplicativos e, desta maneira, depende muito de colaboradores-chave da organização.
  A organização encontra-se no nível 2, repetível, no qual os processos de monitoramento da SI estão padronizados para os ativos críticos, porém ainda são muito dependentes da experiência de alguns colaboradores com habilidade nesse processo.
- Processo Comunicação: A finalidade deste processo é avaliar a efetividade dos canais de comunicação entre todos os atores envolvidos na SI. Para executar este processo, analisa-se a clareza e a completude do processo de transparência que deve ser mantida entre as diversas partes interessadas.
  — Respondente: Existe a padronização nos processos de comunicação da organização. A organização procura documentar todas as comunicações frente à SI e às práticas de comunicação em SI da forma mais ostensiva possível. Contudo, existem dificuldades na reatividade da organização, ocasionando dificuldades em corrigir os desvios que ocorreram no processo de comunicação.
  A organização está no nível 3, processo definido, no qual existe uma padronização, documentação e treinamentos nos processos de comunicação. Existe a formalização de práticas, porém não existe sofisticação nos processos. Ainda são encontradas dificuldades na correção de desvios.
- Processo de Garantia: Este processo busca muita manutenção dos níveis da SI de acordo com o que foi projetado na estratégia e, ainda, o uso dos relatórios e apontamentos dos controles como retroalimentação da estratégia.
  — Respondente: Sendo um órgão público, a estratégia é norteada pelas leis e normas do serviço público que devem ser cumpridas por toda a organização. A manutenção dos níveis acordados ainda é muito dependente do conhecimento de colaboradores isolados.
  A organização está no nível 2, repetível, porém intuitivo – existe uma padronização na manutenção da segurança dos ativos críticos de informação, definido pelo aparato normativo. A confiança está depositada no conhecimento concentrado de colaboradores específicos, podendo ocorrer falhas.

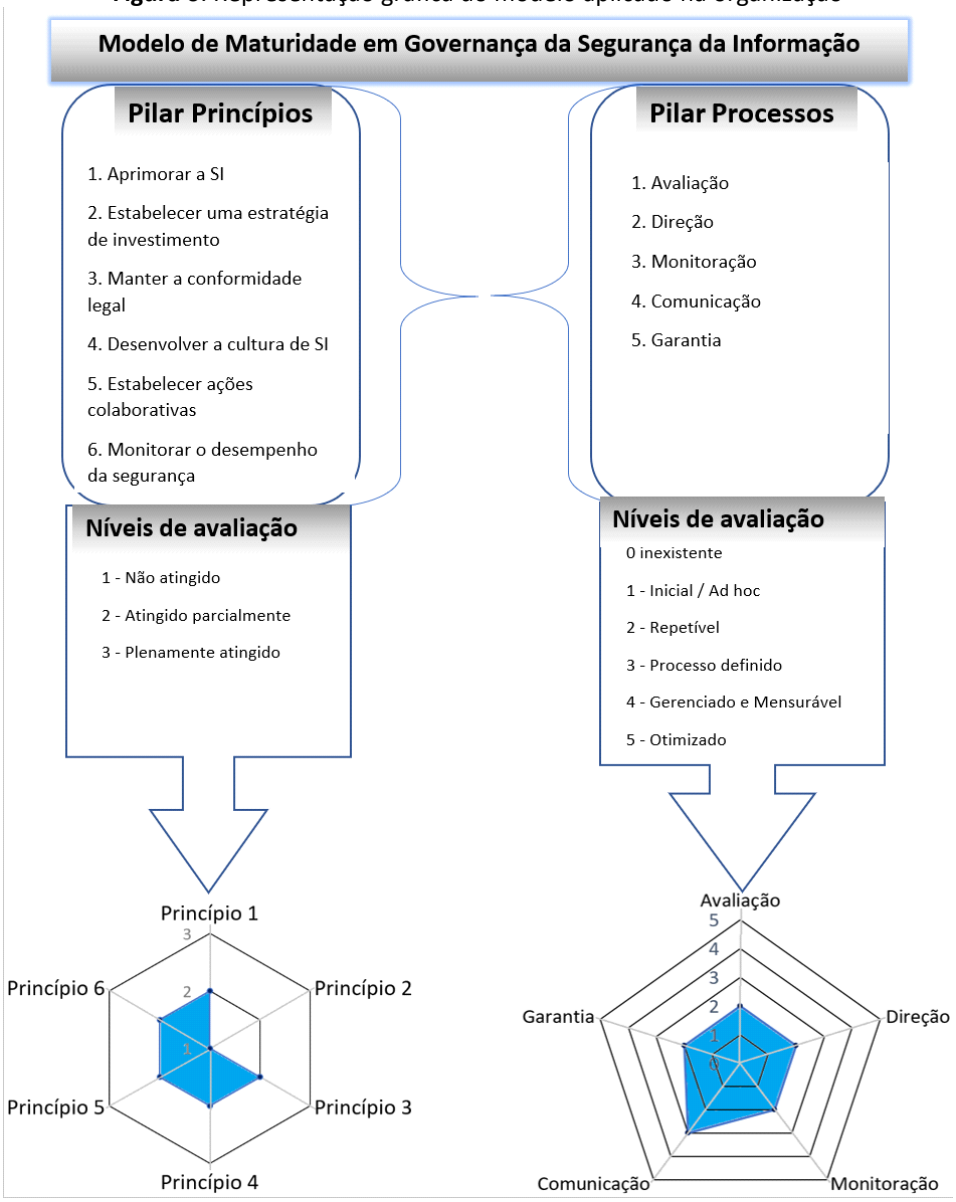
  Conforme mostrado no Quadro 4, os processos direção, avaliação, monitoração e garantia, estão no nível 2, repetível. O processo de comunicação avançou para o nível 3, processo definido, de maturidade, no contexto avaliado.

Quadro 4: Avaliação no Pilar Processos pelo entrevistado

Níveis de Avaliação	Processos				
	Direção	Avaliação	Monitoração	Comunicação	Garantia
0 - Inexistente					
1 - Inicial / Ad hoc					
2 - Repetível, porém intuitivo	X	X	X		X
3 - Processo definido				X	
4 - Gerenciado e Mensurável					
5 - Otimizado					

Fonte: Dados da pesquisa (2024)

Figura 6: Representação gráfica do modelo aplicado na organização



Fonte: os autores

Na figura 6 os dois pilares do modelo são mostrados e questionados nos respectivos níveis de maturidade, sendo produzido um gráfico com o alcance da aplicação do modelo na organização, mostrando um tímido alcance nos níveis de maturidade em GovSI na organização.

8 CONCLUSÃO

No contexto dos órgãos da APF, o levantamento da auditoria (Brasil, 2016), realizada pelo TCU em 376 Instituições da Administração Pública Federal, mostrou a necessidade de maior governança em relação às informações usadas pelas entidades estatais, com destaque para a SI desde a sua produção até o descarte. Tal relatório, orientado pelas leis e normas reguladoras das atividades do Estado que abordam as ameaças à SI, apontam, assim, uma tímida maturidade da GovSI na Administração Pública Federal.

A revisão da literatura mostrou que não há proposta de aplicação de um modelo de maturidade da GovSI na Administração Pública Federal, o que torna difícil a mensuração do atual grau de maturidade de qualquer órgão e que possa, ainda, ser comparado com o grau de maturidade de outros órgãos. Deste modo, o estudo está fundamentado no modelo de GovSI para a Administração Pública (Guimarães, 2016), e a construção e aplicação do modelo desse trabalho.

Dentre as principais limitações encontradas na pesquisa, podem-se apontar a quantidade de respondentes da pesquisa de aderência do modelo proposto e a falta de disponibilidade e abertura dos gestores da APF para aplicação do modelo.

A principal contribuição da pesquisa foi a propositura de um modelo de maturidade em GovSI, aplicável, principalmente na APF, mas não se limita a essas. Com a aplicação do modelo que é embasado em processos e princípios pode-se obter visualmente a maturidade da governança da segurança da informação, com sua medição prática do grau de maturidade da maturidade de GovSI da entidade, comparar com outras que aplicarem, e ainda permitir uma estratégia de evolução dentro dos níveis de maturidade abarcado pelo modelo proposto.

Proposta de trabalho futuros: Especificamente derivados desta pesquisa, 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.

É importante destacar que o modelo proposto neste trabalho não determina os passos necessários para que os graus de maturidade elencados sejam alcançados, o que confere à organização uma maior versatilidade em adequar seus recursos organizacionais dentro de suas limitações, sendo aderente às principais normas e leis e normas dentro do contexto da APF.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013. Técnicas de segurança — Código de prática para controles de segurança da informação. 2013. (ABNTa)

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

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27032:2015. Técnicas de segurança — Diretrizes para segurança. 2015. (ABNTc)

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 18 ago 2018. Seção 1, p. 59.

BRASIL. Tribunal de Contas da União. Governança de Tecnologia da informação (TI) na Administração Pública Federal (APF). Relatório de levantamento TC 008.127/2016-6. Brasília, DF, 2016.

CARCARY, M. et al. A Framework for Information Security Governance and Management. In **IT Professional**, vol. 18, no. 2, p. 22-30, Mar.-Apr. 2016. IEEE Computer Society, 2016. Disponível em: < https://ieeexplore.ieee.org/document/7436688>.

CHRISSIS, Mary Beth; KONRAD, Mike; SHRUM, Sandy. CMMI® for Development, Version 1.3: Improving Processes for Developing Better Products and Services. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2010. Disponível em: https://kilthub.cmu.edu/articles/report/CMMI_for_Development_Version_1_3/6572342/1?file=12057386.

DRUCKER, P. **Gerindo para o Futuro**. 1. ed. Lisboa: Difusão Cultural, 1992.

GUIMARÃES, Rogério. **Modelo de governança de segurança da informação para a Administração Pública Federal**. 2016. 108f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, 2016.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION – ISACA. Capability Maturity Model Integration (CMMI v2). Pensylvania: SEI, 2018.

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION – ISACA. COBIT 4.1: Control Objectives for Information and Related Technologies: ISACA, 2007.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018. Security techniques — Information security management systems -- Overview and vocabulary. 2018.

LAKATOS, E. M. et al. **Metodologia científica**. São Paulo: Atlas S.A., 1991.

MACONACHY, W. V.; SCHOU, C. D. et al. **A Model for Information Assurance**: An Integrated Approach. 2001. IEEE - Workshop on Information Assurance and Security. United States Military Academy, p. 5-6. West Point, New York, 2001. Disponível em: < http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf>.

NICHOLLS, J.; BROWN, L. **Measuring and managing risk culture**. Financial Services Forum. Melbourne. Towers Watson, 2012. Disponível em: <https://www.actuaries.asn.au/Library/Events/FSF/2012/MeasuringAndManagingRiskCulture6CNichollsBrown.pdf>.

OFFICE OF GOVERNMENT COMMERCE — OGC. Information Technology Infrastructure Library - ITIL v3. OGC, 2011.

OLIVEIRA, Roosevelt Benvindo de. **Levantamento de maturidade em gerenciamento de portfólio de projetos em organizações da Administração Pública Federal**. 2017. 62 f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, 2017.

ROSSETI, R. P. C. **Governança Corporativa**: Fundamentos, Desenvolvimento e Tendências. Editora Saraiva, 2007.

SETIAWAN, H.; PUTRA, F. A.; PRADANA, R. P. **Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1**: A case study at communication data

applications of XYZ institute. Information Technology Systems and Innovation -ICITSI, 2017. International Conference on, p. 251-256, 2017. Disponível em: <https://ieeexplore.ieee.org/document/7437689>.

SIQUEIRA, J. **O modelo de maturidade de processos**. Instituto Brasileiro da Qualidade Nuclear – IBQN, 2005. Disponível em: < https://www.abcq.com.br/p/14/o-modelo-de-maturidade-de-processos.html>.

SOFTEX, Melhoria de Processo do Software Brasileiro - MPS.BR 2016. Sociedade Núcleo de Apoio à Produção e Exportação de Software do Rio de Janeiro - RIOSOFT e Sociedade Núcleo (SOFTEX 2000), Rio de Janeiro, 2016.

SOLMS, R. V.; THOMSON, K. L. et al. Information Security Governance control through comprehensive policy architectures. 2011 **Information Security for South Africa**, Johannesburg, p. 1-6, 2011. Disponível em: < https://ieeexplore.ieee.org/document/6027522/>.

SOLMS, V. S.; GCAZA, N. A Strategy for a cybersecurity culture: A South African perspective. **The Electronic Journal of Information Systems in Developing Countries** – EJISDC, p. 1-17, 2017. School of ICT, Nelson Mandela Metropolitan University. South Africa, 2017. Disponível em: < https://onlinelibrary.wiley.com/doi/pdf/10.1002/j.1681-4835.2017.tb00590.x>.

SOLMS, V. S.; GCAZA, N. From information security to cyber security. **Computers & Security**, v. 38, October 2013, Pages 97-102, 2013. Disponível em: < https://www.sciencedirect.com/science/article/pii/S0167404813000801?via%3Dihub#vt1>.

THE WORLD BANK. Governance and development. 1818 H Street, Washington, D.C. (1992). Disponível em:< http://documents.worldbank.org/curated/pt/604951468739447676/Governance-and-development>

TELECOMMUNICATION STANDARDIZATION SECTOR – ITU-T. X.800: Security architecture for Open Systems Interconnection for CCITT Applications. Recommendation. Washington, 2004. Disponível em: <https://www.itu.int/rec/T-REC-X.800-199103-I/en>.

US Department of Energy. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. June 2022. Washington, D.C.: US Department of Energy, 2022. Disponível em:<https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf >

YAOKUMAH, W.; BROWN, S. An Empirical Study into Information Security Governance Focus Areas and their Effects on Risk Management. 2014 ANNUAL GLOBAL ONLINE CONFERENCE ON INFORMATION AND COMPUTER TECHNOLOGY, v. 1, p. 42-49. IEEE Computer Society. Louisville, KY, USA, 2014. Disponível em: < https://ieeexplore.ieee.org/document/7113663>.

Recebido em/Received: 06/07/2023 | Aprovado em/Approved: 01/02/2025