# Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal

**Antonio João Gonçalves de Azambuja**
Universidade Federal do Rio Grande do Sul, Porto Alegre – RS, Brasil.

**João Souza Neto**
Universidade Católica de Brasília, Brasília – DF, Brasil

Este trabalho apresenta um modelo de maturidade de segurança cibernética para os órgãos da administração pública federal. Foi realizada uma pesquisa qualitativa para analisar os modelos de maturidade de segurança cibernética encontrados na literatura, os quais serviram de base para o desenvolvimento do modelo proposto. Para analisar, compreender e interpretar o material qualitativo, os procedimentos técnicos utilizados foram a análise de conteúdo e um questionário *online*. A análise de conteúdo foi dividida na fase de pré-análise, exploração do material e tratamento dos resultados, o que possibilitou a definição dos domínios para o modelo proposto. A aplicação do modelo foi realizada por meio do questionário *online*, com a participação de 35 (trinta e cinco) órgãos da administração pública federal. Os resultados demonstraram que, no geral, há baixa maturidade dos órgãos pesquisados em segurança cibernética. O modelo proposto atende o objetivo VII da estratégia de segurança cibernética, "Elevar o nível de maturidade de Segurança Cibernética na Administração Pública Federal", bem como auxilia no aprimoramento da segurança cibernética no Brasil.

**Palavras-chave:** segurança da informação, segurança cibernética, estratégia de segurança cibernética

**DOI:** https://doi.org/10.21874/rsp.v71i3.3210 **| E- ISSN**: 2357-8017
[Artigo recebido em 07 de fevereiro de 2018 e aceito em 29 de junho de 2020.]

## Modelo de madurez de la seguridad cibernética para los órganos de la administración pública federal

Este trabajo presenta un modelo de madurez de Seguridad Cibernética para los órganos de la Administración Pública Federal Brasileña. Ha sido realizada una investigación cualitativa para analizar los modelos de madurez de Seguridad Cibernética encontrados en la literatura, los cuales han actuado como soporte para el desarrollo del modelo propuesto. Para analizar, comprender e interpretar el material cualitativo, los procedimientos técnicos utilizados fueron el análisis de contenido y una encuesta *online*. El análisis de contenido fue dividido en etapas de preanálisis, exploración del material y tratamiento de los resultados, lo que posibilitó definir los dominios para el modelo propuesto. La aplicación del modelo fue realizada por medio de una encuesta *online*, con la participación de 35 (treinta y cinco) órganos de la Administración Pública Federal. Los resultados demostraron que, en general, hay baja madurez de los órganos investigados en Seguridad Cibernética. El modelo propuesto atiende el objetivo VII de la Estrategia de Seguridad Cibernética, que prevé "Elevar el nivel de madurez de Seguridad Cibernética en la Administración Pública Federal", así como también ayuda a mejorar la Seguridad Cibernética en Brasil.


**Palabras clave:** seguridad de información, seguridad cibernética, estrategia de seguridad cibernética


## Cybersecurity maturity model for the Brazilian Federal Government Agencies

This paper presents a Cybersecurity maturity model for the agencies of the Brazilian Federal Public Administration. Qualitative research was conducted to analyze Cybersecurity maturity models found in the literature, which served as ground to develop the proposed model. To analyze, understand and construe the qualitative material, we used content analysis and an online questionnaire. The content analysis was divided into pre-analysis, material exploration and handling of results which allowed setting the domains of the proposed model. The model was applied through an online questionnaire, with the participation of 35 (thirty-five) agencies of the Brazilian Federal Public Administration. The results evidenced that, in general, the agencies surveyed have low maturity in Cybersecurity. The proposed model meets goal 7 of the Brazilian Cyber Security Strategy, as well as assists in the improvement of Cyber Security in Brazil.


**Keywords:** information security, cybersecurity, cybersecurity strategy

## 1 Introdução

A informação tem se mostrado, atualmente, um ativo de valor para as organizações, talvez o mais precioso dada a sua importância para os negócios. Portanto, deve ser protegida.

Os bens essenciais para o funcionamento de uma sociedade, como as redes de computadores, sistemas de informação, de transporte, financeiros, de saúde, entre outros, estão cada vez mais dependentes da tecnologia da informação (TI) (Rahman *et al*., 2011; Xiao-Juan; Li-Zhen, 2010).

As ações de segurança da informação (SI) têm como objetivo a proteção das informações de vários tipos de ameaças para garantir a continuidade das atividades da organização, minimizar os riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio (Manoel, 2014).

Os princípios básicos da SI são: confidencialidade, integridade e disponibilidade. Esses princípios orientam a análise, o planejamento, a implantação e o controle de segurança para as informações das organizações. A confidencialidade visa limitar o acesso e uso da informação a pessoas autorizadas; a integridade tem como característica proteger as informações contra alterações em seu estado original; e a disponibilidade torna as informações disponíveis para usuários autorizados, quando necessário.

As práticas básicas de segurança cibernética (SegCiber)[1] estão descritas na norma ABNT NBR ISO/IEC 27032:2015, que determina os aspectos comuns da referida atividade e suas ramificações na SI, segurança de redes, segurança da internet e proteção das infraestruturas críticas da informação.

O advento das redes de computadores permitiu que dois ou mais dispositivos sejam conectados entre si, de modo a compartilharem serviços e informações, criando o espaço cibernético (Silva, 2011).

O espaço cibernético constitui novo e promissor ambiente de exposição ao risco, tornando-se necessário implementar ações para assegurar a confidencialidade, a integridade e a disponibilidade das informações das organizações (Killmeyer, 2006).

O Estado brasileiro, entendido como uma organização, também necessita de ações que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações (Mandarino Júnior, 2010).

A SI tem sido objeto de preocupação em todos os levantamentos de governança de TI realizados pelo Tribunal de Contas da União (TCU). O levantamento realizado em 2014, mostrou fragilidades na coordenação e normatização da SI nos órgãos da administração pública federal (APF), o que expõe as organizações a riscos de indisponibilidade de serviços e perda da integridade de informações.

As organizações da APF devem planejar ações que fortaleçam a defesa nacional para mitigar vulnerabilidades que podem ser exploradas com os avanços da tecnologia. É necessário que a prestação de serviços para a sociedade seja realizada sem a exposição excessiva a riscos ou ameaças (Brito, 2011).

Contudo, para avaliar e poder melhorar o nível dos serviços providos, esses órgãos devem realizar um levantamento da sua maturidade quanto aos requisitos sugeridos pelas melhores práticas de SegCiber.

A avaliação de SegCiber nas organizações pode ser realizada por meio de um modelo de maturidade, que fornece um ponto de referência para conhecer o nível de suas práticas, processos e métodos para, então, definir metas e prioridades de melhoria.

Entre as metas descritas na atual estratégia de segurança da informação e comunicações e de segurança cibernética da APF[2], para o período de 2015 e 2018, publicada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), destaca-se como mecanismo de acompanhamento e avaliação de SegCiber nos órgãos da APF, conhecer e implementar o indicador anual do nível de maturidade na área.

Diante do exposto, emerge a seguinte questão de pesquisa: "quais são as características de um modelo de maturidade de SegCiber, que esteja em conformidade com a estratégia de segurança da informação e comunicações e de segurança cibernética da APF?"

Para responder à questão de pesquisa mencionada, este trabalho tem como objetivo geral: contribuir para o aprimoramento da SegCiber no Brasil. E como objetivos específicos: i) identificar na literatura modelos de maturidade de SegCiber; ii) desenvolver o modelo de maturidade de SegCiber conforme a estratégia de segurança da informação e comunicações e de segurança cibernética da APF; e iii) analisar o nível de maturidade de SegCiber das organizações que participarem da pesquisa.

Este artigo busca apresentar o modelo de maturidade de SegCiber para ajudar as organizações públicas a avaliarem o seu estado atual de SegCiber, conforme proposto no objetivo da pesquisa. Para tal, foi construído em 7 (sete) seções.

A seção 1 (um) apresenta a introdução. Na seção 2 (dois) encontra-se a revisão da literatura e na seção 3 (três) o trabalho aborda o problema de pesquisa. Na seção 4 (quatro) são apresentados os conceitos que compõem o referencial teórico. A seção 5 (cinco) discorre sobre os procedimentos metodológicos utilizados na pesquisa.

Na seção 6 (seis) consta uma análise dos modelos de maturidade estudados e a discussão dos resultados da aplicação do modelo proposto no objetivo deste trabalho, com a participação de 35 (trinta e cinco) organizações da APF. Por fim, a seção 7 (sete) apresenta a conclusão do artigo.

## 2 Revisão da literatura

Na revisão da literatura, o tema pesquisado foi modelo de maturidade de SegCiber, com foco no espaço temporal do período de 2007 a 2017. As buscas foram realizadas no portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes[1]), *Google Scholar*[2] e Biblioteca Digital Brasileira de Teses e Dissertações (BDTD[3]), no período de janeiro a março de 2017.

As palavras-chave em inglês na pesquisa foram *Cyber Security* e *Maturity Models*. Já em português as palavras-chave pesquisadas foram: segurança cibernética e modelo de maturidade, conforme se observa nas Tabelas 1 e 2.

**Tabela 1 | Resultados da pesquisa por palavras-chave em inglês**

| Palavras-chave | Capes[1] | Google Scholar[2] | BDTD[3] |
|---|---|---|---|
| *Cyber security* | 11.287 | 26.800 | 0 |
| *Cyber security* and *Maturity models* | 123 | 1.070 | 0 |
| *Cybersecurity* and *Maturity models* | 46 | 704 | 0 |

Fonte: elaboração própria.

**Tabela 2 | Resultados da pesquisa por palavras-chave em português**

| Palavras-chave | Capes[1] | Google Scholar[2] | BDTD[3] |
|---|---|---|---|
| Segurança cibernética | 4 | 428 | 0 |
| Segurança cibernética e modelo de maturidade | 0 | 0 | 2 |

Fonte: elaboração própria.

### 2.1 Análise da revisão da literatura

Nas buscas realizadas foi encontrada uma dissertação de mestrado sobre o Modelo de Capacidades e Maturidade para Defesa Cibernética (Silva, 2011) e outra que aborda uma Metodologia de Identificação de Nível de Maturidade de SegCiber em *Smart Grid* (Machado, 2016).

Silva (2011), em sua dissertação, apresenta um modelo de capacidades de defesa cibernética. Segundo o autor, o modelo de maturidade é importante para apoiar o planejamento estratégico de ações de defesa cibernética. A implantação da defesa cibernética pelo Estado demanda o desenvolvimento de capacidades-chave, entre elas a detecção de ataques, mecanismos de defesa, monitoramento de situação, comando e controle, aprimoramento de estratégias e táticas e desenvolvimento de sistemas.

Machado (2016), por sua vez, apresenta em seu trabalho uma metodologia tendo como base dois grandes pilares: i) o primeiro focado na identificação dos ativos, ameaças e impactos; e ii) o segundo na realização de uma análise e classificação do nível de maturidade. O autor apresenta no seu trabalho uma metodologia de classificação do nível de maturidade de SegCiber nas redes elétricas inteligentes. A identificação da maturidade tem as seguintes etapas: i) a primeira consiste na realização de um levantamento dos ativos, ameaças e impactos; ii) a segunda estabelece processos para assegurar o cumprimento e aplicação dos requisitos de segurança.

Já os artigos relevantes para a pesquisa foram: *Cybersecurity Capability Maturity Models for Provides of Critical Infrastructure* (Muita; Miron, 2014), *A Dynamic Capability Maturity Model for Improving Cyber Security* (Adler, 2013), e *The Community Cyber Security Maturity Model* (White, 2007).

Muita *et al.* (2014), em seu artigo, examinam modelos de maturidade de capacidade de SegCiber para provedores de infraestrutura crítica tais como, sistemas de geração e distribuição de energias, redes de transporte, redes computacionais e tecnologias de informação e comunicação dos governos. Além disso, os autores apontam que faltam informações e conscientização sobre os modelos de maturidade de capacidade de SegCiber mais adequados para uma determinada situação e como devem ser implementados. O trabalho discorre sobre os modelos de maturidade de recursos de SegCiber para identificar padrões e controles disponíveis para fornecedores de infraestrutura crítica.

Adler (2013) apresenta em seu artigo uma descrição sobre desempenho dinâmico e inovador da gestão com a abordagem da SegCiber. O desempenho da gestão descreve como as organizações direcionam os seus recursos para alcançar suas metas e objetivos. Os métodos de desempenho de gestão consistem em: i) medir o desempenho da organização com métricas relevantes; ii) analisar as falhas e definição de metas; iii) desenvolver planos para melhorar o desempenho; e iv) execução dos planos.

Segundo White (2007), as comunidades e governos estão cada vez mais dependentes dos sistemas informatizados e, com isso, cada vez mais vulneráveis a ameaças cibernéticas. A necessidade da preparação para prevenir, detectar e responder a essas ameaças torna a SegCiber um domínio estratégico para as organizações. O autor apresenta em seu artigo

um modelo de maturidade que pode ser utilizado para elaboração de um programa para melhorar a postura de segurança organizacional.

Os 5 (cinco) modelos referenciados apresentam em comum as questões relacionadas com as ameaças, as vulnerabilidades e infraestrutura tecnológica que têm impactos na maturidade de SegCiber das organizações. Os modelos trazem distinções no tocante às práticas de compartilhamento das informações referentes à SegCiber. É essencial uma articulação entre as organizações para estabelecer políticas, diretrizes e normas para obter e disponibilizar as informações de SegCiber, visando mitigar os riscos e aumentar a resiliência operacional.

No que pese o fato da estratégia de segurança da informação e comunicações e de segurança cibernética da APF para o período de 2014-2018 estabelecer entre suas metas avaliar o nível de maturidade de SI e SegCiber para os órgãos da APF, na pesquisa bibliográfica não foram identificados trabalhos que apresentassem os resultados da referida avaliação para elevar a maturidade de SegCiber da APF. Essa é uma lacuna importante, pois sem essa avaliação as organizações não conhecerão suas fragilidades e não poderão elaborar planos de ação para saná-las.

No levantamento bibliográfico, a disponibilidade de dissertações e artigos é reduzida na combinação dos termos *Cyber Security* e *Maturity Model*, demonstrando uma lacuna na literatura sobre o tema. Na pesquisa bibliográfica, demonstra-se que são poucas as referências teóricas direcionadas à elaboração e à aplicação de um modelo de maturidade de SegCiber.

## 3 Problema de pesquisa

Na concepção científica, problema é qualquer questão não resolvida e que é objeto de discussão, em qualquer domínio do conhecimento. (Gil, 2010).

As repetidas ameaças cibernéticas em organizações de todos os setores, tipos e tamanhos demonstram a necessidade da implementação de práticas, métodos e processos relacionados com a SegCiber. A falta de maturidade de SegCiber nas organizações resulta nos seguintes problemas:

- falta de conformidade com leis, regulamentos e normas aplicadas à SI (ITGI, 2006);
- perdas financeiras relacionadas a incidentes cibernéticos (PWC, 2016);
- falta de confidencialidade das informações restritas (BRASIL, 2015);
- falta de integridade das informações (BRASIL, 2015);
- indisponibilidade do acesso às informações (BRASIL, 2015);
- vazamento de informações (BRASIL, 2015); e
- perda de informação (BRASIL, 2015).

Sendo assim, dado o significativo impacto dessas consequências nas organizações, importa conhecer o nível de maturidade de SegCiber nas mesmas.

## 4 Referencial teórico

O referencial teórico visa apresentar o suporte necessário para apoiar esta pesquisa. Desta forma, serão abordados a seguir os fundamentos teóricos para o entendimento do conteúdo da referida pesquisa.

### 4.1 Segurança da informação

A definição do termo Segurança da Informação pode ser encontrada na norma ABNT NBR ISO/IEC 27002:2013, que diz: a SI é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos.

Para a *Information Systems Audit and Control Association* (ISACA, 2012), a SI deve proteger as informações contra divulgação não autorizada, alterações em seu estado original e manter a disponibilidade das informações quando for solicitada, e com isso assegurar a confidencialidade, integridade e disponibilidade.

Os atributos confidencialidade, integridade e disponibilidade são os principais e que melhor definem as propriedades para assegurar a gestão de SI (Killmeyer, 2006). Os referidos atributos são definidos pelo autor da seguinte forma: i) confidencialidade: proteção das informações contra acesso não autorizado, independente da forma como ela é armazenada ou local de armazenamento; ii) integridade: é a proteção de informações, aplicações, sistemas e redes contra mudanças intencionais, não autorizadas ou acidentais; e iii) disponibilidade: é a garantia de que as informações e os recursos estão acessíveis pelos usuários autorizados, conforme a necessidade.

### 4.2 Segurança cibernética

A estratégia de segurança da informação e comunicações e de segurança cibernética da APF (Brasil, 2015), define a SegCiber como a arte de assegurar a existência da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas.

O espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas e organizacionais, constituindo um novo território, por vezes conhecido e desconhecido, a ser desbravado pelos bandeirantes do século 21 (Machado, 2016).

A falta de práticas, processos e métodos para assegurar a proteção do espaço cibernético, seus ativos e suas infraestruturas críticas podem impactar a segurança do Estado e da sociedade, mudando a percepção da SegCiber no mundo, direcionando a uma reflexão de como estão evoluindo as atividades de guerra cibernética.

A defesa cibernética é um conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os sistemas de informação (Brasil, Ministério da Defesa, 2010).

Os conceitos de segurança são complementares. Dentro de uma abordagem clássica dos estudos de SegCiber, a perspectiva do conceito de segurança está relacionada diretamente com a capacidade do Estado para assegurar a sua sobrevivência (Agostini, 2014).

No entanto, segundo Agostini (2014), nos anos 1950 os estudos de segurança perderam seu carácter exclusivo militar. Nos anos 1990, com o crescimento da internet, observou-se uma ampliação da agenda de estudos no referido tema, com a inserção de discussões sobre segurança humana, ambiental, econômica e cibernética.

Sendo a SegCiber uma inquietação dos setores de defesa e estratégia do Estado, a agenda de estudos sobre o tema transborda a abordagem clássica de segurança. Nesse sentido, vale citar a contribuição do *Copenhagen Peace Research Institute*[3] (Copri) para o campo teórico, a qual ressalta que a presença do discurso de ações de SegCiber, por si só, não garante o efetivo processo de segurança do Estado (Silva, 2013).

Diante dos estudos elaborados pelo Copri sobre os estágios de securitização, é possível identificar que o Estado brasileiro tem direcionado ações para ciberdefesa[4] e cibersegurança[5] (Nunes, 2012).

### 4.3. Estratégia de Segurança da Informação e Comunicações e SegCiber da APF

O documento é um instrumento de apoio ao planejamento estratégico governamental que reúne um conjunto de objetivos e metas para o período de 2015 a 2018, elaborado pelo GSI/PR.

Considerando que são atividades essenciais para o Estado, essa estratégia tem como objetivo a articulação e coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento das ações de segurança e resiliência das infraestruturas críticas, dos serviços de Estado e a mitigação dos riscos aos quais encontram-se expostas as organizações e a sociedade (Brasil, 2015).

A estratégia ressalta que não obstante os esforços do governo em fortalecer as ações de SI e de SegCiber, o que inclui o arcabouço de normas complementares publicadas

pelo GSI/PR desde 2008, no geral, os níveis de maturidade dos órgãos da APF ainda se encontram em patamar aquém do desejado (Brasil, 2015).

Segundo essa estratégia os órgãos da APF devem estabelecer, considerando o planejamento organizacional, ações de avaliação anual, bem como ações para o desenvolvimento de mecanismos internos de acompanhamento e avaliação sistemática do nível de maturidade, visando à excelência nas áreas de segurança da informação e comunicações (SIC) e SegCiber, prevenção e o combate de crimes cibernéticos no Governo Federal.

### 4.4 Norma ISO/IEC 27032:2015

A Norma ISO/IEC 27032:2015 estabelece diretrizes para melhorar o estado de SegCiber, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.

A SegCiber, como abordada na norma, busca a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço. Define como ciberespaço um ambiente complexo resultante da interação de pessoas, *software* e serviços da internet por meio de dispositivos tecnológicos e redes conectadas a ele, sem formato físico.

### 4.5 Modelos de maturidade

Um modelo de maturidade funciona como um guia para a organização conhecer o seu estado atual e realizar um plano de melhoria, na busca da excelência (Oliveira, 2006).

Becker *et al.* (2009) estabelecem que um modelo de maturidade tem 2 (dois) componentes: i) o meio de medir e descrever o desenvolvimento de um objeto, mostrando a progressão hierárquica; e ii) os critérios para medir os processos.

A importância da aplicação dos modelos de maturidade destacada por Kernezer (2006) refere-se à descoberta de oportunidades de melhoria no gerenciamento de

projetos, identificação das mudanças necessárias para a melhoria da maturidade e dependência tecnológica que as organizações possuem.

Assim sendo, para propor o modelo de maturidade de SegCiber conforme a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, este trabalho considerou os seguintes modelos de maturidade, a saber:

#### 4.5.1 *Capability Maturity Model*

O *Capability Maturity Model* (CMM) é uma marca registrada do *Software Enginnering Institute* (SEI) da Universidade *Carnegie Mellon*, em Pittsburg, nos Estados Unidos da América (EUA).

É um modelo para avaliação da maturidade dos processos de *software* de uma organização. Tem como objetivo a melhoria dos processos utilizados pelas organizações de desenvolvimento e manutenção de sistemas, para minimizar os erros relacionados ao desenvolvimento, planejamento e aperfeiçoamento dos sistemas informatizados.

Está organizado em 5 (cinco) níveis crescentes de maturidade definidos em áreas-chave de um processo de *software,* detalhados em práticas que devem ser cumpridas na sua implantação. As práticas descrevem o que deve ser realizado, exigindo documentos, treinamentos e definição de políticas. Os níveis de maturidade do modelo CMM são:

- Inicial (1): pobremente controlado e imprevisível.
- Repetitivo (2): pode repetir as tarefas executadas com sucesso.
- Definido (3): processo é caracterizado e bem entendido.
- Gerenciado (4): processo é medido e controlado.
- Otimizado (5): foco na melhoria contínua do processo.

### *4.5.2 Capability Maturity Model Integration (CMMI)*

É um modelo evolutivo do CMM, criado pelo SEI, para integrar estruturas de processos de melhorias demandadas pelas organizações. Segundo o SEI (2002), o CMMI estabelece a diferença entre os conceitos de organização e empresa, a valorização, validação e evolução dos processos de verificação.

Está dividido em 5 (cinco) níveis: inicial, gerenciado, definido, quantitativamente gerenciado e otimizado. Os níveis fazem parte das áreas de processos, que possuem um conjunto de metas específicas e genéricas. As características de comprometimento com a execução, habilitação para a execução, direcionamento para a implementação e verificação da implementação fazem parte das metas genéricas. Já as metas com foco no negócio são classificadas como específicas (Sei, 2002).

### *4.5.3 Cybersecurity Capability Maturity Model*

O *Cybersecurity Capability Maturity Model* (C2M2, 2014) pode ajudar as organizações de todos os setores, tipos e tamanhos, a avaliar e fazer melhorias em seus programas de SegCiber. O foco está na implementação de práticas de gestão de segurança associadas aos ativos de TI e às operações de tecnologia. As organizações podem usar esse documento para os seguintes fins:

- fortalecer as capacidades de SegCiber;
- permitir a avaliação de forma eficaz e consistente do estado atual da SegCiber;
- compartilhar conhecimento, melhores práticas e referências de SegCiber; e
- permitir a priorização das ações e investimentos para melhorar a SegCiber.

O modelo apresenta uma metodologia de autoavaliação nas organizações, visando à identificação dos seus níveis de maturidade e as melhorias a serem realizadas no programa de SegCiber. A autoavaliação fornece informações aos seguintes atores: gestores responsáveis pela tomada de decisão; responsáveis pela gestão de recursos e operações organizacionais; responsáveis pela aplicação da autoavaliação; e facilitadores da aplicação de autoavaliação.

Para medir a progressão, os modelos de maturidade têm tipicamente níveis de maturidade em uma escala numérica. O C2M2 usa uma escala de 4 (quatro) níveis, que permite à organização definir o seu estado atual de SegCiber, determinar o seu futuro e identificar os recursos necessários para alcançar esse estado futuro.

Os níveis do C2M2 são os seguintes:

- Nível 0: não contém práticas para um domínio.
- Nível 1: contém um conjunto de práticas iniciais para um domínio.
- Nível 2: representa o nível inicial para institucionalização das atividades em um domínio. Contém um conjunto de práticas que são sustentadas ao longo do tempo.
- Nível 3: as atividades em um domínio foram institucionalizadas e estão sendo gerenciadas.

O modelo está organizado em 10 (dez) domínios, com práticas agrupadas por objetivos, conforme o Quadro 1.

**Quadro 1 | Domínios vs Objetivos**

| Domínio | Objetivos |
|---|---|
| Gestão de risco | Estabelecer a estratégia da gestão risco;<br>Gerenciar o risco cibernético;<br>Gestão das atividades. |
| Gestão de ativos, mudanças e configurações | Gerenciar o inventário de ativos;<br>Gerenciar a configuração de ativos;<br>Gerenciar as alterações de ativos;<br>Atividades de gestão. |
| Gestão de identidade e acesso | Estabelecer e manter identidades;<br>Controlar o acesso;<br>Atividades de gestão. |
| Gestão de ameaças e vulnerabilidades | Identificar e responder às ameaças;<br>Reduzir as vulnerabilidades;<br>Atividades de gestão. |

| Domínio | Objetivos |
|---|---|
| Consciência situacional | Realizar registro de *log's;*<br>Realizar monitoramento;<br>Estabelecer e manter uma estrutura operacional;<br>Atividades de gestão. |
| Compartilhamento de informações e comunicações | Compartilhar informações;<br>Atividades de gestão. |
| Resposta a eventos, incidentes e continuidade de operações | Detectar eventos;<br>Escalar eventos e declarar incidentes;<br>Responder a incidentes e eventos escalados;<br>Plano de continuidade;<br>Atividades de gestão. |
| Cadeia de suprimentos e gerenciamento de dependências externas | Identificar dependências;<br>Gerenciar o risco da dependência;<br>Atividades de gestão. |
| Gerenciamento da força de trabalho | Atribuir responsabilidades;<br>Controlar o ciclo de vida da força de trabalho;<br>Desenvolver a força de trabalho;<br>Aumentar a conscientização em SegCiber;<br>Atividades de gestão. |
| Gestão do programa de SegCiber | Estabelecer a estratégia do programa;<br>Patrocinar o programa;<br>Estabelecer e manter a arquitetura de SegCiber;<br>Desenvolver *software* seguro;<br>Atividades de gestão. |

**Fonte: C2M2 (2014) – Adaptado pelos autores**

O relatório da autoavaliação identifica para cada domínio e objetivos as lacunas no desempenho nas práticas do modelo. A etapa inicial da análise dos resultados determina se essas lacunas são importantes para a organização. Após a análise, a organização prioriza as ações necessárias para implementar as práticas não atendidas na primeira avaliação, para, com isso, alcançar um nível de maturidade mais elevado.

### *4.5.4 NIST Cybersecurity Framework*

Este modelo foi desenvolvido em resposta a uma ordem executiva do Presidente dos EUA, Barack Obama, em fevereiro de 2013, para reforçar a resiliência da infraestrutura crítica daquele país e manter um ambiente cibernético que encorajasse a eficiência, inovação e prosperidade econômica (Presidente, 2013).

O *NIST Cybersecurity Framework* (2014) permite que as organizações apliquem os princípios e as melhores práticas de gestão de risco para aprimorar a SegCiber e a resiliência das infraestruturas críticas, com as seguintes funções e objetivos:

- Identificar: desenvolver a compreensão organizacional para gerenciar o risco de sistemas, ativos, dados e recursos.
- Proteger: desenvolver e implementar as salvaguardas adequadas para assegurar os serviços de infraestrutura crítica.
- Detectar: desenvolver e implementar as atividades apropriadas para identificar a ocorrência de eventos de SegCiber.
- Responder: desenvolver e implementar as atividades apropriadas para tomar medidas relativas a eventos de SegCiber detectados.
- Recuperar: desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido aos eventos de SegCiber.

Os níveis e objetivos são:

- Parcial – nível 1: as práticas de gerenciamento referentes a SegCiber não são formalizadas e os riscos são gerenciados de forma *ad-hoc*.
- Informado – nível 2: as práticas de gerenciamento referentes a SegCiber são aprovadas pela alta administração, mas não podem ser estabelecidas como políticas de toda a organização.
- Repetido – nível 3: as práticas de gerenciamento referentes a SegCiber são formalmente aprovadas e expressas como política.
- Adaptado – nível 4: a organização adapta suas práticas de SegCiber com base nas lições aprendidas e indicadores preditivos derivados de atividades anteriores e atuais de SegCiber. Por meio de processo de melhoria contínua, incorpora tecnologias avançadas e práticas de SegCiber.

O modelo apresenta a seguinte descrição para cada um dos processos:

- Gerenciamento de riscos: processo contínuo de identificação, avaliação e resposta ao risco. Para gerir os riscos, as organizações devem compreender a probabilidade de que um evento ocorra e o seu impacto resultante.

- Programa integrado de gerenciamento de risco: processo de conscientização do risco de SegCiber no nível organizacional com abordagem de toda a organização para gerenciar o risco, o que permite o compartilhamento das informações referentes à segurança para toda a organização.

- Participação externa: processo de integração com as organizações do ambiente de atuação, compartilhamento das informações com parceiros para assegurar que informações atuais e precisas são utilizadas para melhorar a SegCiber.

#### *4.5.5 The Community Cyber Security Maturity Model*

O *The Community Cyber Security Maturity Model* (CCSMM), proposto por White (2007), fornece uma estrutura que as comunidades e os estados podem usar para determinar seu nível de preparação para criar um plano para melhorar sua postura de SegCiber. Os elementos do modelo são os seguintes: enfrentar as ameaças; definir métricas; compartilhar informações e tecnologias.

O CCSMM reconhece a necessidade de organizações terem métricas tecnológicas para desenvolver um programa de SegCiber, como também exercitar testes de capacidade de segurança, implementar atividades de treinamento e compartilhamento das informações relacionadas com a SegCiber.

Níveis do modelo:

- Nível 1: a conscientização sobre as ameaças relacionadas com a SegCiber está estabelecida e não estruturada.

- Nível 2: os processos estão em desenvolvimento para melhorar e tratar as questões relacionadas com a SegCiber.

- Nível 3: os processos e mecanismos estão implementados para identificar eventos relevantes de SegCiber.
- Nível 4: os processos estão desenvolvidos para estabelecer métodos mais adequados e proativos para detectar e responder ataques.
- Nível 5: os processos para detectar e responder qualquer tipo de ataque estão implementados.

## 5 Metodologia

Esta pesquisa classifica-se como Pesquisa Aplicada, quanto à sua natureza. Este tipo de pesquisa objetiva gerar conhecimento para aplicação prática, dirigida à solução de problemas específicos.

Com relação à forma de abordagem do problema, foi realizada uma pesquisa qualitativa para analisar, compreender e interpretar os modelos de maturidade de SegCiber encontrados na revisão da literatura, que foram a base para o desenvolvimento do modelo de maturidade de SegCiber para APF, ora proposto.

Do ponto de vista dos objetivos, a pesquisa é exploratória, já que foi realizada uma avaliação dos modelos de maturidade de SegCiber disponíveis na literatura.

Para analisar, compreender e interpretar o material qualitativo, os procedimentos técnicos utilizados foram um questionário *online* e a análise de conteúdo.

O questionário, como instrumento de pesquisa, permite a obtenção de dados ou informações sobre as características ou as opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo (Fonseca, 2002).

O *link* de acesso ao questionário *online* foi encaminhado por *e-mail* para gestores de SI de 35 (trinta e cinco) órgãos da APF. O referido instrumento de pesquisa tem 9 (nove) domínios, 33 (trinta e três) objetivos, 56 (cinquenta e seis) práticas para o nível 1, 111 (cento e onze) práticas para o nível 2 e 117 (cento e dezessete) práticas para o nível 3.

Cada prática corresponde a 1 (uma) pergunta, sendo assim, o questionário tem um total de 284 (duzentos e oitenta e quatro) perguntas.

As perguntas são objetivas com possibilidade somente de 1 (uma) resposta "sim" ou "não", ou "não tenho informações suficientes para responder". O questionário foi elaborado com a ferramenta de formulários do *Google*[6], a qual permite implementar o seguinte fluxo: conforme a resposta de determinada prática para um determinado nível o participante é direcionado para a prática seguinte do nível mais elevado.

Sendo assim, o participante terá possibilidade de responder às perguntas relacionadas ao Nível 2, se tiver respondido "sim" para as práticas do Nível 1 de determinado domínio. O tempo médio para responder o questionário é de 20 (vinte) minutos.

Por sua vez, segundo Bardin (2011), a análise de conteúdo representa um conjunto de técnicas de análise de comunicações que visam obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) dessas mensagens (Bardin, 2011).

A análise de conteúdo, conforme Bardin (2011), prevê 3 (três) fases: i) pré-análise, com as seguintes sub-fases: leitura sobre o tema; seleção do material; representatividade do material; homogeneidade e pertinência do material; ii) exploração do material; e iii) tratamento dos resultados, inferência e interpretação.

**5.1 Descrição da pesquisa**

Considerando o método de Bardin (2011), a pesquisa foi dividida em fases. Na primeira, pré-análise, foi realizada a revisão da literatura e a seleção do material utilizado como base de apoio teórico para a pesquisa.

Na segunda, foram organizados os dados dos modelos em domínios, identificando as categorias e as unidades de registro. A terceira consistiu no tratamento dos resultados que, para Bardin (2011), compreende a inferência e a interpretação.

[6] Formulários do *Google*: ferramenta que você pode coletar e organizar informações em pequena ou grande quantidade. Gratuitamente.

### 5.2 Análise de conteúdo

Este estudo analisou os seguintes modelos *Capability Maturity Model, Capability Maturity Model Integration, Cybersecurity Capability Maturity Model, NIST Cybersecurity Framework* e *The Community Cyber Security Maturity Model.*

#### 5.2.1 Pré-análise

A fase de pré-análise visa à organização do material da pesquisa, sistematizar as ideias iniciais e desenvolver um plano de análise. Segundo Bardin (2016), é nessa fase que o pesquisador escolhe os documentos que serão analisados, esclarece as hipóteses, define os objetivos e estabelece os indicadores para fundamentar a interpretação final.

Na referida fase foi realizada a revisão da literatura, leitura crítica, seleção e organização do material, identificação dos relacionamentos dos pontos relevantes e comuns entre os modelos utilizados como base de apoio teórico para a pesquisa.

#### 5.2.2 Exploração do material

A fase de exploração do material consiste na definição das categorias, identificação das unidades de registro visando à categorização e à contagem de frequência das unidades de contexto nos documentos Bardin (2016).

Para o autor, essa fase possibilita ou não a riqueza das interpretações e inferências, sendo assim, a codificação, a classificação e a categorização são requisitos básicos na fase de exploração do material.

#### 5.2.3 Tratamento dos resultados

A definição dos temas permitiu o agrupamento em nove domínios, para o modelo proposto, conforme a similaridade identificada entre os temas na análise de conteúdo.

Os domínios do modelo proposto são: gestão de riscos; gestão de ativos; gestão de acesso; gestão de ameaças e vulnerabilidades; gestão de continuidade; compartilhamento de informações; capacitação, conscientização e cultura; infraestrutura tecnológica; e governança de SegCiber.

## 6 Análise e discussão dos resultados

Dando prosseguimento ao estudo e atendendo aos objetivos geral e específicos declarados na introdução, esta seção apresenta uma análise dos modelos estudados e os resultados da aplicação do modelo de maturidade de SegCiber proposto.

### 6.1 Análise

Para propor o modelo de maturidade de SegCiber para os órgãos da APF, foi realizado um estudo dos modelos de maturidade descritos no referencial teórico deste trabalho. Com a análise de conteúdo foi possível identificar a similaridade dos domínios, elementos, processos, objetivos e práticas dos modelos estudados.

Na análise comparativa entre os modelos que contribuíram para esta pesquisa, destaca-se que eles têm foco nas organizações de forma global, não se preocupando com as características relacionadas com a SegCiber para órgãos do setor público.

Segundo Carvalho *et al.* (2003), os modelos de maturidade diferem no que se refere aos níveis de abstração, no entanto, apresentam a possibilidade de relacionamentos entre os seus domínios e se complementam com base nos temas abordados.

O modelo C2M2 (2014) tem como temas: gestão de risco de SegCiber, gestão de ativos, gestão de acesso, gestão de ameaças e vulnerabilidades, resposta a eventos de SegCiber, gestão de continuidade, compartilhamento de informações, cultura de SegCiber, infraestrutura tecnológica e governança de SegCiber.

Já o modelo *NIST Cybersecurity Framework* (2014) tem similaridade com o C2M2 (2014) nos seguintes temas: gestão de risco de SegCiber, compartilhamento de informações e cultura de SegCiber. E o modelo CCSMM (2007) tem similaridade com os dois modelos selecionados nos seguintes temas: gestão de ameaças e vulnerabilidades, compartilhamento de informações, cultura de SegCiber e infraestrutura tecnológica.

O Quadro 2 apresenta os temas abordados nos modelos de maturidade com maior similaridade entre si, identificados durante a análise de conteúdo.

**Quadro 2 | Temas dos modelos de maturidade**

| Temas | C2M2 | *NIST Cybersecurity Framework* | *The Community Cyber Security Maturity Model* |
|---|---|---|---|
| Gestão de risco de SegCiber | X | X | |
| Gestão de ativos | X | | |
| Gestão de acesso | X | | |
| Gestão de ameaças e vulnerabilidades | X | | X |
| Resposta a evento de SegCiber | X | | |
| Gestão de continuidade | X | | |
| Compartilhamento de informações | X | X | X |
| Cultura de SegCiber | X | X | X |
| Infraestrutura tecnológica | X | | X |
| Governança de SegCiber | X | | |

Fonte: elaboração própria.

Diante do referido contexto, o Quadro 3 apresenta o percentual de alinhamento dos modelos que apresentaram maior similaridade entre os seus domínios, os quais contribuíram para definição dos 9 (nove) domínios do modelo proposto por este trabalho.

**Quadro 3 | Domínio do modelo proposto vs modelos analisados**

| Domínios do modelo proposto | Relacionamento dos domínios dos modelos com os domínios do modelo proposto | | |
|---|---|---|---|
| | C2M2 | *NIST Cybersecurity Framework* | *The Community Cyber Security Maturity Model* |
| Gestão de risco | X | X | |
| Gestão de ativos | X | | |
| Gestão de acesso | X | | |
| Gestão de ameaças e vulnerabilidades | X | | X |
| Gestão de continuidade | X | | |
| Compartilhamento de informações | X | X | X |
| Capacitação, conscientização e cultura | X | X | X |
| Infraestrutura tecnológica | X | | X |
| Governança de SegCiber | X | | |
| Percentual dos relacionamentos dos domínios com os modelos | 47,36% (9) | 15,78% (3) | 21,05% (4) |

Fonte: elaboração própria.

O modelo do C2M2 (2014) contribuiu com 9 (nove) domínios, o modelo do *NIST Cybersecurity Framework* (2014) com 3 (três) e o modelo *The Community Cyber Security Maturity Model* (CCSMM), elaborado por White (2007), com 4 (quatro).

No Quadro 3, é possível identificar que o maior percentual de alinhamento dos domínios do modelo proposto ocorre com os domínios do C2M2[7] (2014), com um percentual de 47,36%, contra 15,78% para o modelo do *NIST Cybersecurity Framework*[8] (2014) e 21,05% para o modelo CCSMM[9] (2007).

A seguir, apresenta-se a matriz de avaliação dos modelos de maturidade (Quadro 4) que apoiam esta pesquisa, com as seguintes variáveis: i) escopo do modelo; ii) tipo de organização; iii) temas abordados; e iv) níveis de maturidade.

**Quadro 4 – Matriz de avaliação dos modelos**

| Matriz/Modelo | C2M2 | *NIST Cybersecurity Framework* | *The Community Cyber Security Maturity Model* |
|---|---|---|---|
| Escopo do modelo | Avaliar e fazer melhorias em seus programas de SegCiber | Aplicar os princípios e as melhores práticas de gestão de risco para aprimorar a SegCiber e a resiliência das infraestruturas críticas | Preparar um plano para melhorar sua postura de SegCiber. Implementar atividades de treinamento e compartilhamento das informações relacionadas com a SegCiber. |
| Tipo de organização | De qualquer setor | De infraestruturas críticas | Não especifica |
| Temas abordados | Riscos, ativos, acesso, ameaças, vulnerabilidades, resposta, continuidade, compartilhamento, cultura, infraestrutura tecnológica | Risco, compartilhamento e cultura | Ameaças, vulnerabilidades, compartilhamento, cultura e infraestrutura tecnológica |
| Níveis de maturidade | 1, 2 e 3 | 1, 2, 3 e 4 | 1, 2, 3, 4 e 5 |

Fonte: elaboração própria.

Na continuidade da análise dos modelos estudados, cabe aqui uma descrição dos aspectos relacionados com os níveis de maturidade presentes nos modelos que contribuíram para esta pesquisa.

Os níveis de maturidade são utilizados para medir a competência organizacional ou maturidade de um conjunto reconhecido das melhores práticas. Os modelos de maturidade têm tipicamente níveis de maturidade em uma escala numérica (C2M2, 2014).

Seguem os aspectos relacionados aos níveis de maturidade:

- Os níveis de maturidade são aplicados para todos os domínios de um modelo. Uma organização pode estar no Nível 2 para determinado domínio e Nível 1 para outro domínio.
- Para uma organização ter a progressão de um determinado nível para um superior, deverá executar todas as práticas nesse nível e seu(s) antecessor(es);
- Visando alcançar um determinado nível, estabelecer uma meta é uma estratégia eficaz para aplicação do modelo.
- As práticas para alcançar determinado nível devem estar alinhadas com os objetivos do negócio e as estratégias de SegCiber.
- As organizações devem avaliar os custos para alcançar os níveis de maturidade mais elevados.

O Quadro 5 apresenta a escala para cada um dos níveis de maturidade do modelo proposto nesta pesquisa, com a descrição das práticas.

**Quadro 5 | Escala dos níveis de maturidade**

| Níveis / Práticas / Descrição | |
|---|---|
| N-0: Não contém práticas para um domínio | |
| Não tem práticas | - |
| N-1: Contém um conjunto de práticas iniciais para um domínio | |
| Tem um conjunto de práticas iniciais, que podem ser realizadas *ad hoc* | A realização da prática depende da iniciativa ou experiência de um indivíduo ou equipe, sem a formalidade de um plano documentado. A qualidade das atividades depende da experiência do indivíduo ou equipe. Neste nível as lições aprendidas não são documentadas e apresentam dificuldade de repetição da melhoria da organização; |
| N-2: Representa um nível de institucionalização das atividades em um domínio | |
| As práticas são documentadas | As práticas de um domínio estão sendo documentadas, com planejamento para atender as necessidades dos objetivos da organização; |

| | |
|---|---|
| As partes interessadas da prática são identificadas e envolvidas | As partes interessadas são identificadas e envolvidas no desempenho das práticas. Pode incluir partes interessadas de dentro ou de fora da organização; |
| Os recursos necessários (pessoas, financiamento e ferramentas) para apoiar os processos são fornecidos | Os recursos são fornecidos na forma de pessoas, financiamento e ferramentas para que as práticas sejam realizadas conforme o planejamento. A implementação de uma prática está relacionada com a disponibilidade ou escassez de recurso. Se todas as práticas tiverem sido implementadas os recursos necessários foram disponibilizados; |
| Os padrões e/ou diretrizes para orientar a implementação das práticas estão identificados | A organização identifica padrões e/ou diretrizes para implementação de práticas de um domínio; |
| N-3: As atividades em um domínio foram institucionalizadas e estão sendo gerenciadas | |
| As atividades são orientadas por políticas, diretrizes e governança | As atividades gerenciadas de um domínio recebem orientação organizacional seguindo as políticas, diretrizes e governança; |
| As políticas incluem requisitos de conformidade para padrões e/ou diretrizes específicas | As práticas seguem requisitos de conformidade com os padrões e/ou diretrizes estabelecidas; |
| As atividades são revisadas periodicamente para garantir a conformidade com a política | A organização realiza periodicamente a revisão das atividades para manter o alinhamento da conformidade com a política; |
| Responsabilidade e autoridade para executar as práticas estabelecidas para a equipe | São estabelecidas as responsabilidades e autoridade para realizar as práticas definidas; |
| A equipe que realiza as práticas tem competências e conhecimento adequado | A equipe possui qualificação para realizar as práticas definidas para um domínio. |

Fonte: C2M2 (2014) – Adaptado pelos autores.

### 6.1.1 Domínios do modelo de maturidade de SegCiber proposto

Cada um dos 9 (nove) domínios do modelo proposto contém um conjunto estruturado de objetivos e práticas de SegCiber relacionados com os níveis de maturidade estabelecidos.

Os objetivos dos domínios compreendem um conjunto de práticas, que são ordenadas por nível de maturidade. Um conjunto de práticas representa as atividades

que uma organização pode realizar para implementar e desenvolver a capacidade de maturidade em um domínio (C2M2, 2014).

O modelo proposto fornece uma orientação para medir e melhorar a maturidade de SegCiber das organizações com base nos padrões existentes. No Quadro 6 está apresentado o exemplo do domínio gestão de riscos que tem as seguintes práticas e objetivos:

**Quadro 6 | Domínio gestão de riscos**

| Objetivo: estabelecer a estratégia de gestão de riscos | |
|---|---|
| Nível | Práticas |
| N-0 | Não tem práticas; |
| N-1 | As práticas de gestão de riscos são aprovadas pela alta administração;<br>As práticas de gestão de riscos são estabelecidas como políticas da organização; |
| N-2 | A estratégia de gestão de riscos está documentada;<br>A estratégia de gestão de riscos oferece uma abordagem para priorização dos riscos, considerando os seus impactos; |
| N-3 | A organização define critérios de risco para avaliar, categorizar e priorizar os riscos operacionais com base no impacto, tolerância e resposta ao risco;<br>A estratégia de gestão de riscos é periodicamente atualizada para representar o atual ambiente de ameaças;<br>Uma classificação de risco específica da organização é documentada e utilizada nas atividades de gestão de riscos. |
| Objetivo: gerenciar o risco de SegCiber | |
| Nível | Práticas |
| N-0 | Não tem práticas; |
| N-1 | Os riscos de SegCiber são identificados;<br>Os riscos identificados são mitigados ou aceitos ou tolerados ou transferidos; |
| N-2 | Os riscos são identificados e avaliados conforme a estratégia de gestão de riscos;<br>Os riscos identificados são documentados;<br>Os riscos identificados são analisados para priorizar as atividades de resposta conforme a estratégia de gestão de riscos;<br>Os riscos identificados são monitorados conforme a estratégia de gestão de riscos;<br>A análise de risco é realizada na arquitetura de rede; |
| N-3 | O programa de gestão de riscos define e estabelece políticas e procedimentos de gestão de risco que apóiam a estratégia de gestão de riscos;<br>A arquitetura de SegCiber é utilizada para realizar a análise de risco;<br>Um repositório estruturado de riscos identificados é utilizado para apoiar as atividades de gestão de riscos. |

| Objetivo: realizar atividades de gestão | |
|---|---|
| Nível | Práticas |
| N-0 | Não tem práticas; |
| N-1 | As práticas são realizadas de forma individual e sem formalidade; |
| N-2 | As práticas documentadas são seguidas nas atividades de gestão de riscos;<br>As partes interessadas das atividades de gestão de riscos são identificadas e envolvidas;<br>Os recursos necessários para apoiar as atividades de gestão de riscos são fornecidos;<br>Os padrões e/ou diretrizes para orientar as atividades de gestão de riscos são identificados; |
| N-3 | As atividades de gestão de riscos são orientadas por políticas e/ou diretrizes organizacionais;<br>As políticas de gestão de riscos incluem requisitos de conformidade com os padrões e/ou diretrizes estabelecidas;<br>As atividades de gestão de riscos são revisadas periodicamente para assegurar sua conformidade com as políticas;<br>A responsabilidade e autoridade para a execução das atividades de gestão de riscos são atribuídas à equipe;<br>A equipe que realiza as atividades de gestão de riscos possui as habilidades e conhecimentos referente às suas atribuições e responsabilidades. |

Fonte: C2M2 e NIST (2014) – Adaptado pelos autores.

Segue uma breve descrição dos domínios do modelo proposto:

- Gestão de riscos: fornece uma orientação para analisar e priorizar o risco e definir a tolerância ao risco.
- Gestão de ativos: realiza a gestão adequada de todos os ativos, evita a perda de informações, otimiza as atividades do negócio, assegura a confiabilidade, integridade e disponibilidade da informação.
- Gestão de acesso: propõe a criação e gerenciamento de identidades para acesso lógico e físico aos ativos de informação. Práticas inadequadas de gerenciamento de acesso podem levar ao uso, divulgação, modificação e destruição não autorizada da informação.
- Gestão de ameaças e vulnerabilidades: visa estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder a ameaças e vulnerabilidades de SegCiber.
- Gestão de continuidade: procura estabelecer e manter planos, procedimentos e tecnologias para detectar, analisar e responder a eventos de SegCiber para sustentar as operações da organização.

- Compartilhamento de informações: busca estabelecer e manter relações com entidades internas e externas para coletar e compartilhar informações sobre SegCiber.
- Capacitação, conscientização e cultura: implementa uma cultura de SegCiber na organização e um plano de capacitação para a força de trabalho.
- Infraestrutura tecnológica: requer uma infraestrutura com mecanismos tecnológicos para identificar, tratar e responder as ameaças e vulnerabilidades de forma integrada.
- Governança de SegCiber: visa estabelecer e manter um programa corporativo de SegCiber que forneça governança, planejamento estratégico e patrocínio para as atividades de SegCiber.

### 6.1.2 Estrutura do modelo de maturidade de SegCiber proposto

As práticas para cada um dos domínios estão agrupadas por objetivos que apoiam a estrutura do modelo. Na Tabela 1 estão apresentados os domínios, os objetivos e as práticas para os seus respectivos níveis de maturidade.

**Tabela 1 | Domínios vs Objetivos vs Práticas vs Níveis de Maturidade**

| Domínios / Objetivos | Número de práticas | | | |
|---|---|---|---|---|
| | Nível 0 | Nível 1 | Nível 2 | Nível 3 |
| Gestão de riscos | | | | |
| Estabelecer a estratégia de gestão de riscos | Não tem práticas | 2 | 2 | 3 |
| Gerenciar o risco de SegCiber | | 2 | 5 | 3 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Gestão de ativos | | | | |
| Gerenciar inventário de ativos | | 1 | 2 | 2 |
| Gerenciar a configuração de ativos | | 1 | 1 | 2 |
| Gerenciar as mudanças nos ativos | | 2 | 2 | 2 |
| Realizar atividades de gestão | | 1 | 4 | 5 |

| Domínios / Objetivos | Número de práticas | | | |
|---|---|---|---|---|
| | Nível 0 | Nível 1 | Nível 2 | Nível 3 |
| Gestão de acesso | | | | |
| Estabelecer e manter identidades | Não tem práticas | 3 | 3 | 1 |
| Controlar acesso | | 3 | 3 | 3 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Gestão de ameaças e vulnerabilidades | | | | |
| Identificar e responder a ameaças | | 3 | 3 | 3 |
| Reduzir as vulnerabilidades de SegCiber | | 3 | 5 | 6 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Gestão de continuidade | | | | |
| Detectar eventos de SegCiber | | 2 | 2 | 3 |
| Escalar eventos e classificar incidentes de SegCiber | | 3 | 4 | 2 |
| Responder a incidentes e eventos escalados de SegCiber | | 3 | 4 | 5 |
| Elaborar e manter plano de continuidade | | 3 | 4 | 4 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Compartilhamento de informações | | | | |
| Compartilhar informações sobre SegCiber | | 2 | 5 | 4 |
| Realizar atividades de gestão | | 1 | 4 | 6 |
| Capacitação, conscientização e cultura | | | | |
| Atribuir responsabilidades de SegCiber | | 2 | 2 | 3 |
| Controlar o ciclo de vida da força de trabalho | | 2 | 2 | 4 |
| Desenvolver a força de trabalho de SegCiber | | 1 | 3 | 5 |
| Aumentar a conscientização em SegCiber | | 1 | 2 | 2 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Infraestrutura tecnológica | | | | |
| Realizar e monitorar as atividades operacionais | | 2 | 4 | 5 |
| Estabelecer e manter um painel operacional padrão | | 1 | 3 | 3 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Governança de segurança cibernética | | | | |
| Estabelecer a estratégia do programa de SegCiber | | 1 | 5 | 1 |
| Patrocinar o programa de SegCiber | | 2 | 6 | 3 |
| Estabelecer e manter a arquitetura de SegCiber | | 1 | 2 | 1 |
| Realizar o desenvolvimento de software seguro | | 1 | 1 | 1 |
| Realizar atividades de gestão | | 1 | 4 | 5 |
| Totais: 9 domínios, 33 objetivos | 0 | 56 | 111 | 117 |

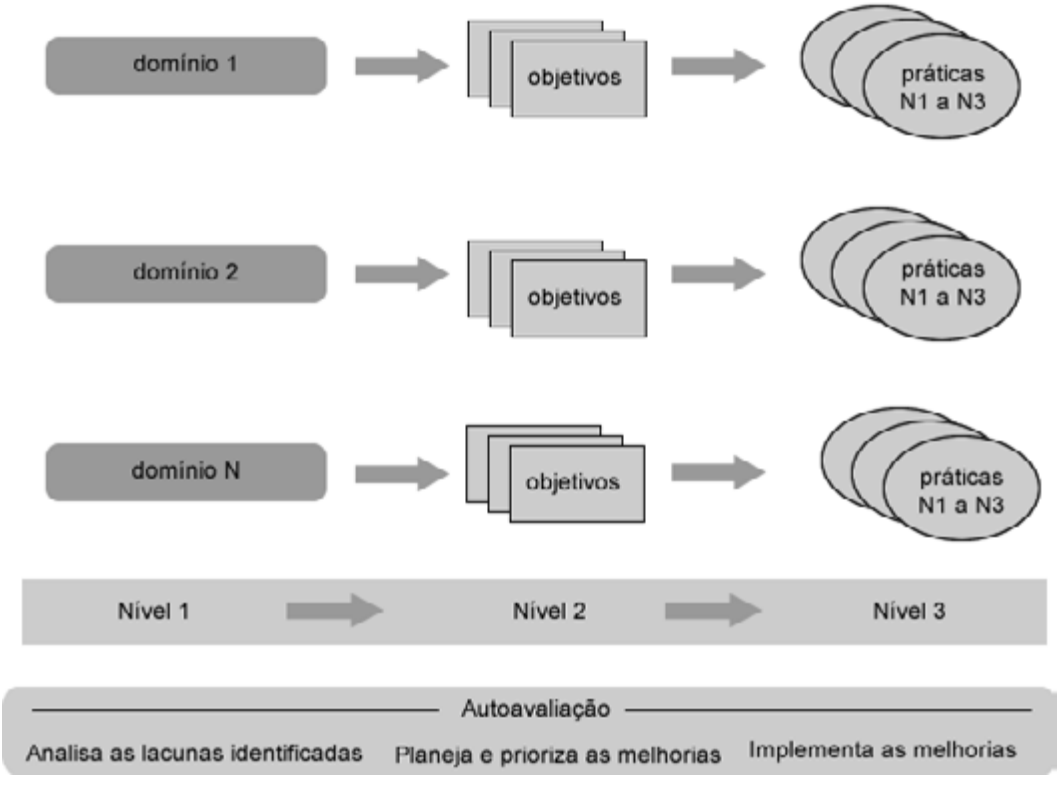
Fonte: elaboração própria.

Para realizar a avaliação da maturidade de SegCiber dos órgãos da APF, foi construído um questionário *online* com os domínios, objetivos e práticas que devem ser implementados pela organização para identificação do seu nível de maturidade. A avaliação permite a identificação das lacunas na maturidade da organização.

A aplicação do modelo demanda que a organização selecione um gestor de SI que esteja familiarizado com a SegCiber da instituição, e tenha, também, conhecimento para ajudar a organização a entender os seus objetivos e realizar um planejamento para atingir níveis mais elevados de maturidade.

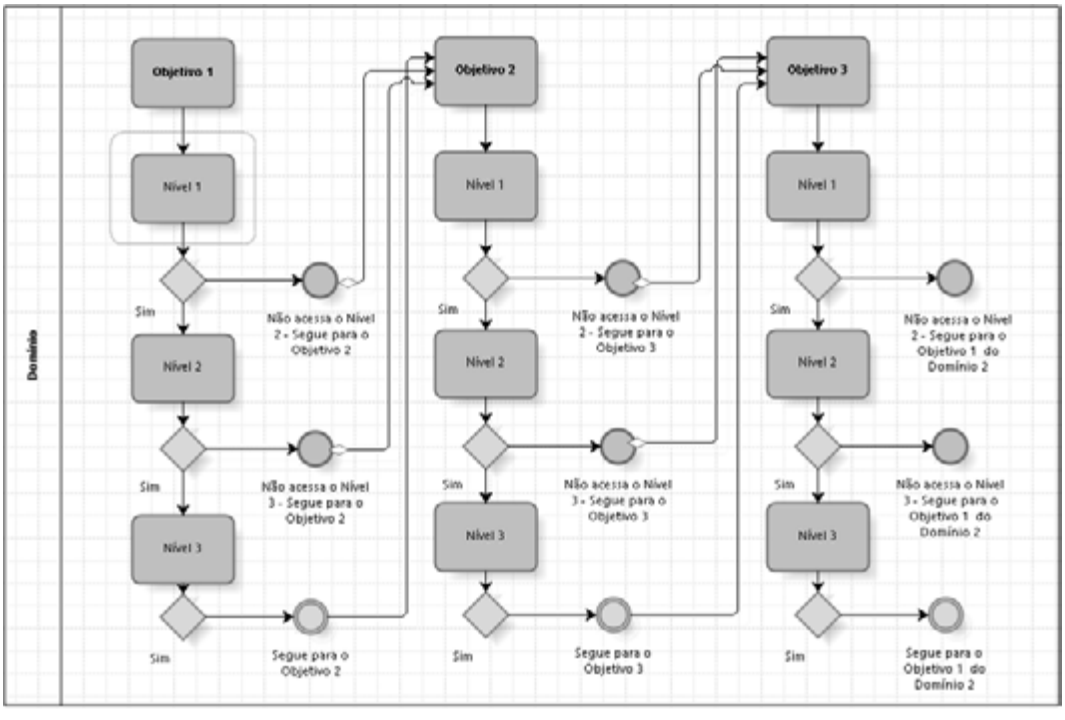
A Figura 1 resume a estrutura do modelo e a Figura 2 apresenta o fluxo da avaliação dentro de um domínio.

**Figura 1 | Estrutura do modelo**




Fonte: Adler (2013) – Adaptado pelos autores.

**Figura 2 | Fluxo da avaliação dentro de um domínio**




Fonte: elaboração própria.

### 6.1.3 Alinhamento do modelo proposto com a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF

A SIC e a SegCiber são estratégicas para a Nação, cabendo à APF direcionar esforços para alcançar os objetivos estabelecidos no documento (Brasil, 2015).

Para tanto, o modelo proposto neste trabalho busca manter alinhamento entre os seus domínios e os objetivos da estratégia. O Quadro 7 apresenta o relacionamento entre os domínios e objetivos.

**Quadro 7| Domínios do modelo vs Objetivos da Estratégia de SIC e SegCiber**

| Domínios | Objetivos |
|---|---|
| Gestão de riscos | Elevar o nível de maturidade de SIC e de SegCiber na APF; |
| Gestão de ativos | |
| Gestão de acesso | |
| Gestão de ameaças e vulnerabilidades | |
| Gestão de continuidade | Valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação; |
| Compartilhamento de informações | Garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF;<br>Ampliar e fortalecer ações colaborativas em SIC e SegCiber com a academia, setores público, privado e terceiro setor no país e no exterior; |
| Capacitação, conscientização e cultura | Garantir continuamente o aprimoramento do quadro de pessoal da APF em SIC e SegCiber de forma qualitativa e quantitativa;<br>Promover mecanismos de conscientização da sociedade sobre SIC e SegCiber; |
| Infraestrutura tecnológica | Valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação; |
| Governança de segurança cibernética | Instituir modelo de Governança Sistêmica de SIC e de SegCiber na APF;<br>Alinhar o planejamento de SIC e de SegCiber ao planejamento estratégico dos órgãos da APF. |

Fonte: elaboração própria.

## 6.2 Discussão dos resultados

Para aplicação do modelo, foram selecionados 35 (trinta e cinco) órgãos da APF, que devem assegurar a confidencialidade, integridade e disponibilidade das suas informações, garantindo a proteção dos seus ativos de informação e das suas infraestruturas críticas.

Os participantes da pesquisa responsáveis pelas respostas das perguntas do questionário *online,* encaminhado por *e-mail*, foram os gestores de SI das organizações, profissionais envolvidos com as questões de SI e que pesquisam e estudam questões de SI.

Com a tabulação das respostas, foi possível elaborar a Tabela 2, a qual apresenta o percentual das organizações por nível, para cada um dos objetivos dos domínios do modelo do proposto.

**Tabela 2 | Percentuais dos objetivos**

| Domínios | Percentuais | | | |
|---|---|---|---|---|
| | Nível 0 | Nível 1 | Nível 2 | Nível 3 |
| Gestão de Riscos | | | | |
| Estabelecer a estratégia de gestão de risco | 43,75 | 18,75 | 12,50 | 25,00 |
| Gerenciar o risco de SegCiber | 31,25 | 37,50 | 18,75 | 12,50 |
| Realizar atividades de gestão | 31,25 | 12,50 | 25,00 | 31,25 |
| Gestão de Ativos | | | | |
| Gerenciar inventário de ativos | 31,25 | 43,75 | 6,25 | 18,75 |
| Gerenciar a configuração de ativos | 56,25 | 18,75 | 6,25 | 18,75 |
| Gerenciar as mudanças nos ativos | 56,25 | 18,75 | 12,50 | 12,50 |
| Realizar atividades de gestão | 43,75 | 31,25 | 6,25 | 18,75 |
| Gestão de Acesso | | | | |
| Estabelecer e manter identidades | 31,25 | 43,75 | 6,25 | 18,75 |
| Controlar acesso | 56,25 | 18,75 | 6,25 | 18,75 |
| Realizar atividades de gestão | 56,25 | 18,75 | 12,50 | 12,50 |
| Gestão de Ameaças e Vulnerabilidades | | | | |
| Identificar e responder a ameaças | 43,75 | 31,25 | 6,25 | 18,75 |
| Reduzir as vulnerabilidades de SegCiber | 43,75 | 12,50 | 31,25 | 12,50 |
| Realizar atividades de gestão | 43,75 | 31,25 | 12,50 | 12,50 |
| Gestão de Continuidade | | | | |
| Detectar eventos de SegCiber | 37,50 | 31,25 | 6,25 | 25,00 |
| Escalar eventos e classificar incidentes de SegCiber | 68,75 | 6,25 | 12,50 | 12,50 |
| | Nível 0 | Nível 1 | Nível 2 | Nível 3 |

| Domínios | Percentuais | | | |
|---|---|---|---|---|
| Responder a incidentes e eventos escalados de SegCiber | 37,50 | 37,50 | 12,50 | 12,50 |
| Elaborar e manter plano de continuidade | 43,75 | 31,25 | 12,50 | 12,50 |
| Realizar atividades de gestão | 50,00 | 25,00 | 6,25 | 18,75 |
| Compartilhamento de Informações | | | | |
| Compartilhar informações sobre SegCiber | 37,50 | 25,00 | 12,50 | 25,00 |
| Realizar atividades de gestão | 43,75 | 31,25 | 0,00 | 25,00 |
| Capacitação, Conscientização e Cultura | | | | |
| Atribuir responsabilidades de SegCiber | 37,50 | 18,75 | 25,00 | 18,75 |
| Controlar o ciclo de vida da força de trabalho | 31,25 | 25,00 | 31,25 | 12,50 |
| Desenvolver a força de trabalho de SegCiber | 56,25 | 25,00 | 6,25 | 12,50 |
| Aumentar a conscientização em SegCiber | 37,50 | 31,25 | 12,50 | 18,75 |
| Realizar atividades de gestão | 50,00 | 31,25 | 0,00 | 18,75 |
| Infraestrutura Tecnológica | | | | |
| Realizar e monitorar as atividades operacionais | 31,25 | 12,50 | 25,00 | 31,25 |
| Estabelecer e manter um painel operacional padrão | 68,75 | 0,00 | 12,50 | 18,75 |
| Realizar atividades de gestão | 43,75 | 25,00 | 18,75 | 12,50 |
| Governança de segurança cibernética | | | | |
| Estabelecer a estratégia do programa de SegCiber | 68,75 | 6,25 | 12,50 | 12,50 |
| Patrocinar o programa de SegCiber | 68,75 | 0,00 | 12,50 | 18,75 |
| Estabelecer e manter a arquitetura de SegCiber | 62,50 | 6,25 | 12,50 | 18,75 |
| Realizar o desenvolvimento de *software* seguro | 68,75 | 6,25 | 0,00 | 25,00 |
| Realizar atividades de gestão | 43,75 | 25,00 | 18,75 | 12,50 |

Fonte: elaboração própria.

Os resultados apresentados na Tabela 2 indicam que as organizações estão dando ênfase ao gerenciamento dos riscos, em detrimento da estratégia de riscos da organização, visto que a maioria das organizações está no Nível 0 para este domínio. No domínio gestão de ativos, as organizações que estão no Nível 0, 35% delas, não podem assegurar a confiabilidade, integridade e disponibilidade da informação.

No domínio gestão de ameaças e vulnerabilidades um elevado número de organizações no Nível 0, com um total de 44%, demonstra que as ameaças não são identificadas, analisadas e tratadas.

Para o domínio gestão de continuidade, que teve como resultado da avaliação 68,75% das organizações no Nível 0 para o objetivo "escalar eventos e incidentes de SegCiber", foi demonstrado que não existem nas organizações critérios para classificar os eventos de segurança e para determinar quando eles devem ser escalados.

É fundamental a articulação entre os órgãos da APF para o compartilhamento de informações relacionadas com a SegCiber. Estabelecer e manter políticas e diretrizes para obter e disponibilizar as informações de SegCiber, incluindo ameaças e vulnerabilidades, são essenciais para mitigar os riscos e aumentar a resiliência operacional.

No domínio compartilhamento de informações, 41% das organizações estão no Nível 0, significando que não possuem práticas para o compartilhamento das informações. Com relação ao domínio capacitação, conscientização e cultura, o número de organizações que não desenvolve a força de trabalho de SegCiber é elevado, 56,25% das organizações pesquisadas. As organizações não atendem às práticas do Nível 1 no domínio infraestrutura tecnológica, ficando grande parte delas no Nível 0, o que significa que essas organizações não possuem um painel operacional para a gestão da infraestrutura tecnológica.

O maior número das organizações está no Nível 0 no domínio governança de SegCiber, o que reforça a necessidade de implementar a governança de SegCiber nos órgãos da APF, em consonância com o objetivo IV da Estratégia de SegCiber, que propõe estabelecer um modelo de Governança de SIC e SegCiber na APF.

Complementando a discussão dos resultados da pesquisa, os Gráficos de número 1 (um) ao número 10 (dez) têm como objetivo apresentar os percentuais dos níveis de maturidade das organizações participantes da pesquisa.

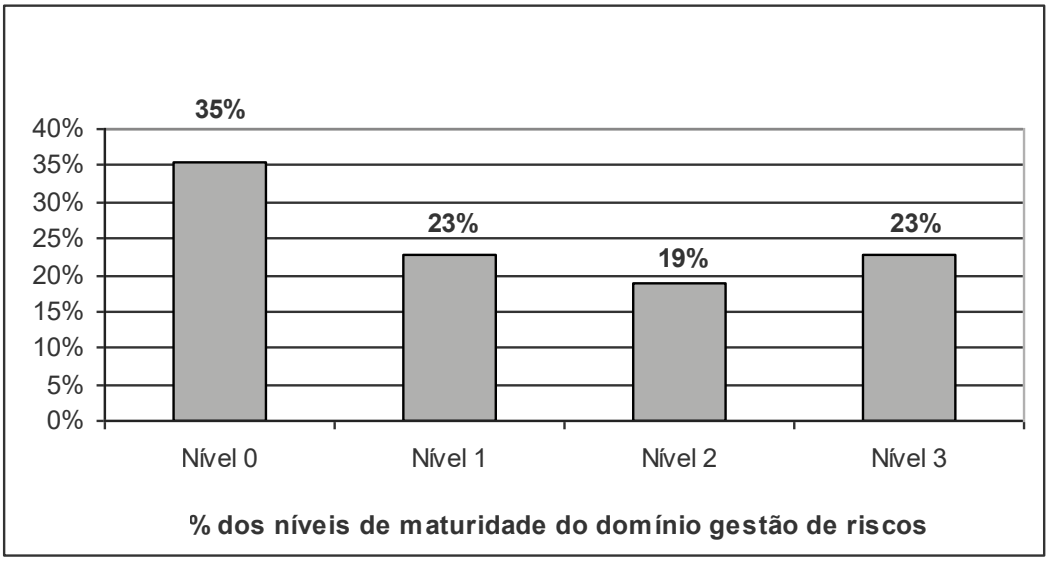
Os percentuais dos dados coletados com a aplicação do questionário *online* estão descritos a seguir para cada um dos 9 (nove) domínios do modelo proposto.

### 6.2.1 Domínio gestão de riscos

Para este domínio, 35% das organizações estão no Nível 0, ou seja, não realizam práticas de gestão de riscos. O elevado número de organizações no Nível 0 demonstra a falta de uma estratégia de gestão de riscos de SegCiber.

O Gráfico 1 apresenta os percentuais dos níveis de maturidade das organizações para o referido domínio.

**Gráfico 1 – Níveis de maturidade para o domínio gestão de riscos**



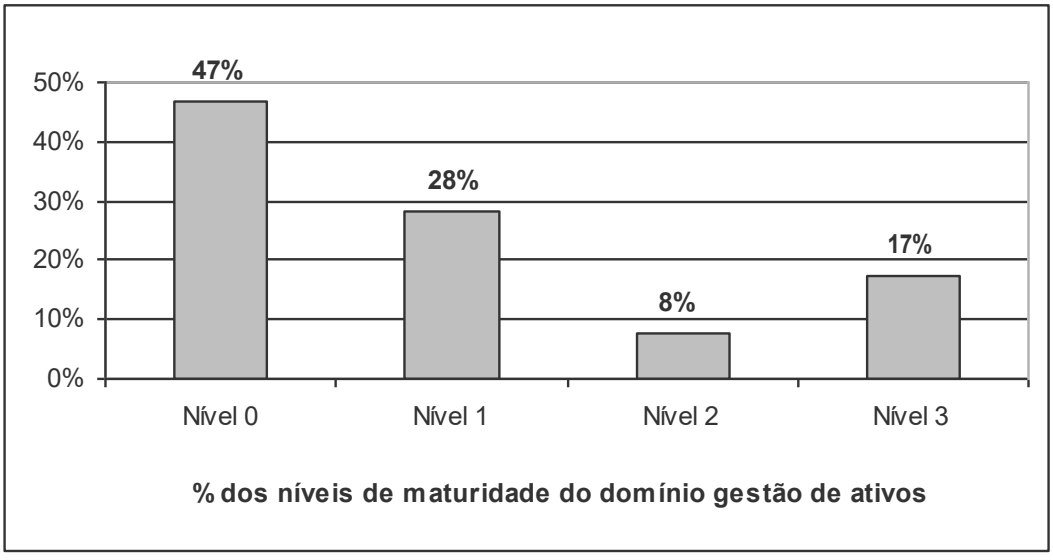

Fonte: elaboração própria.

### 6.2.2 Domínio gestão de ativos

Neste domínio, o percentual de organizações no Nível 0 foi de 47%, maior que no domínio gestão de riscos. Com a falta de maturidade neste domínio, a organização não consegue assegurar a confiabilidade, integridade e disponibilidade da informação, uma vez que a realização de uma gestão adequada dos ativos evita a perda de informações e otimiza as atividades do negócio.

O Gráfico 2 apresenta os percentuais dos níveis de maturidade das organizações para o domínio gestão de ativos.

**Gráfico 2 | Níveis de maturidade para o domínio gestão de ativos**

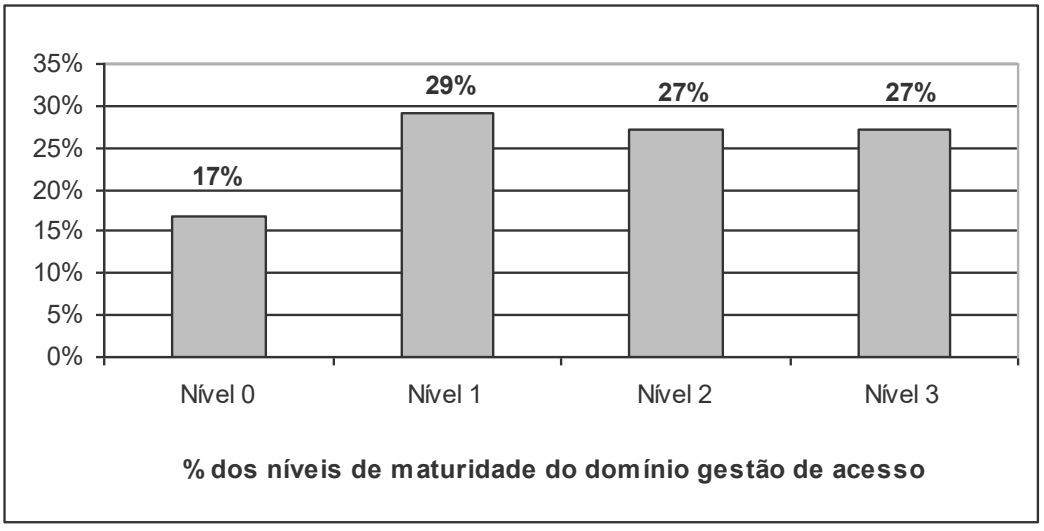



Fonte: elaboração própria.

### 6.2.3 Domínio gestão de acesso

Os resultados do domínio gestão de acesso, apresentados no Gráfico 3, são os que têm o menor percentual de organizações no Nível 0 em comparação com os demais. O fato da maioria das organizações estar nos Níveis 1, 2 e 3 demonstra que existe, por parte das organizações, controles de acesso lógico relacionados com os sistemas de informação e controles de acesso físico às instalações.

**Gráfico 3 | Níveis de maturidade para o domínio gestão de acesso**

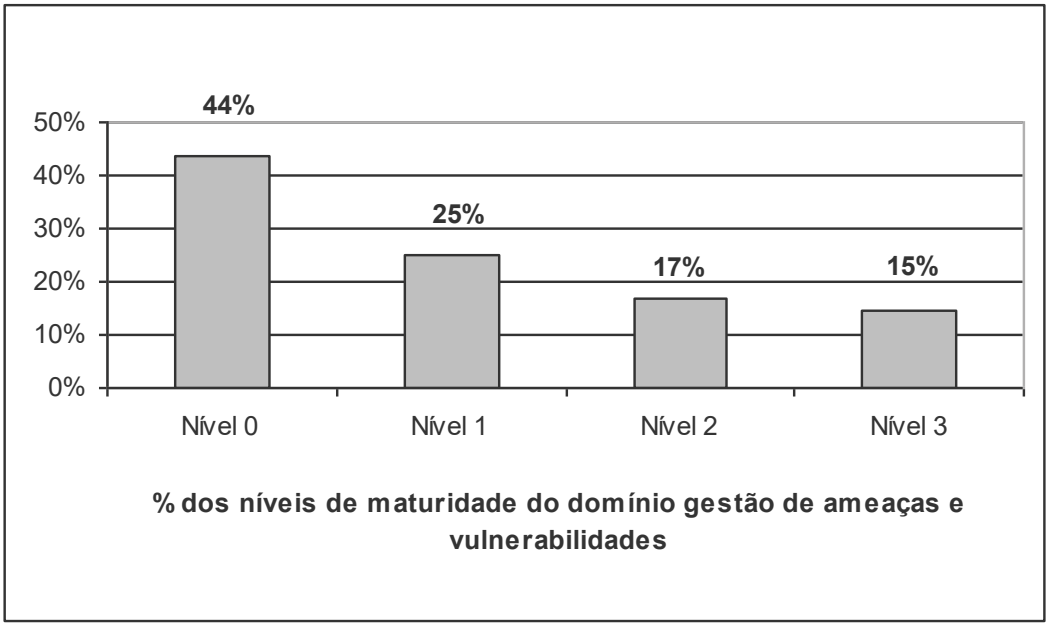



Fonte: elaboração própria.

### 6.2.4 Domínio gestão de ameaças e vulnerabilidades

Os percentuais obtidos para o domínio gestão de ameaças e vulnerabilidades estão apresentados no Gráfico 4. O maior número das organizações está no Nível 0 para este domínio. Essas organizações não possuem práticas para este domínio, o que torna difícil e oneroso detectar, identificar, analisar, gerenciar e responder às ameaças e vulnerabilidades de SegCiber.

**Gráfico 4 – Níveis de maturidade para o domínio gestão de ameaças e vulnerabilidades**

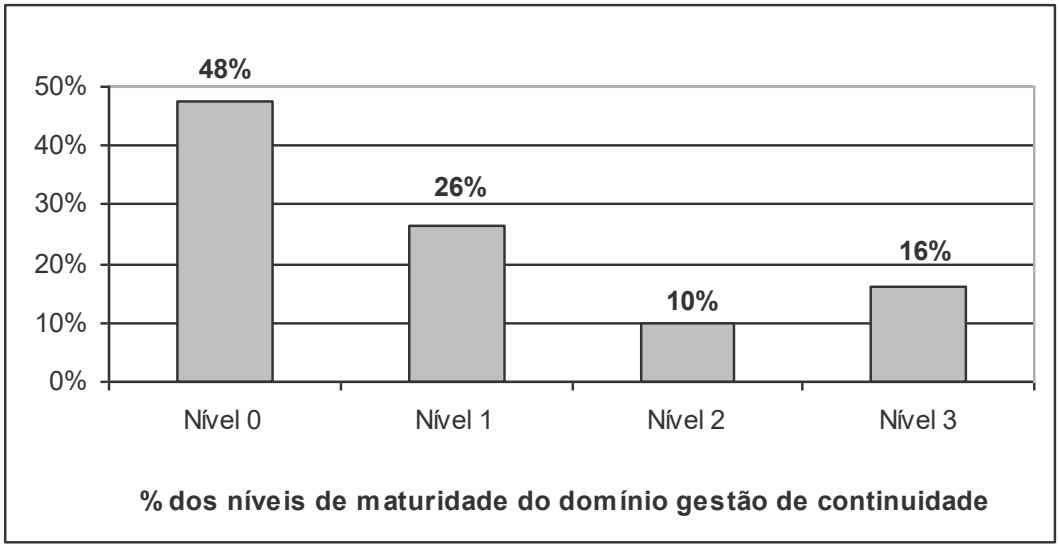



Fonte: elaboração própria.

### 6.2.5 Domínio gestão de continuidade

Os níveis de maturidade das organizações para o domínio gestão de continuidade apresentaram os seguintes percentuais: 48% (Nível 0), 26% (Nível 1), 10% para o (Nível 2) e 16% (Nível 3). Estes percentuais podem ser visualizados no Gráfico 5. A pouca maturidade para este domínio demonstra que as organizações não possuem planos, procedimentos e tecnologias para sustentar as operações das organizações como resposta a eventos de SegCiber.

**Gráfico 5 | Níveis de maturidade para o domínio gestão de continuidade**

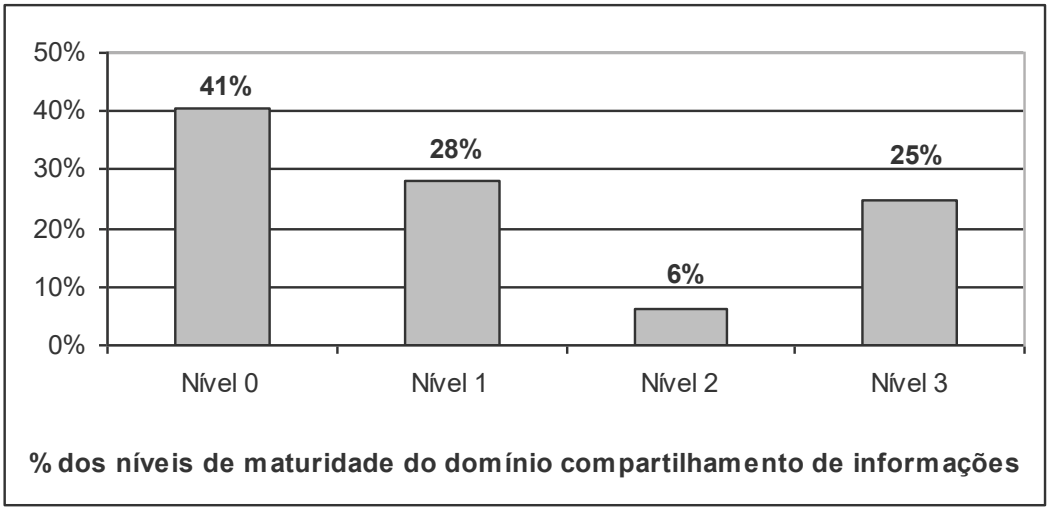



Fonte: elaboração própria.

### 6.2.6 Domínio compartilhamento de informações

O maior número das organizações está no Nível 0 para o domínio compartilhamento de informações. O compartilhamento de informações é um instrumento para aumentar o conhecimento para enfrentar as ameaças e vulnerabilidades (White, 2007). O Gráfico 6 apresenta os percentuais para este domínio.

**Gráfico 6 | Níveis de maturidade para o domínio compartilhamento de informações**

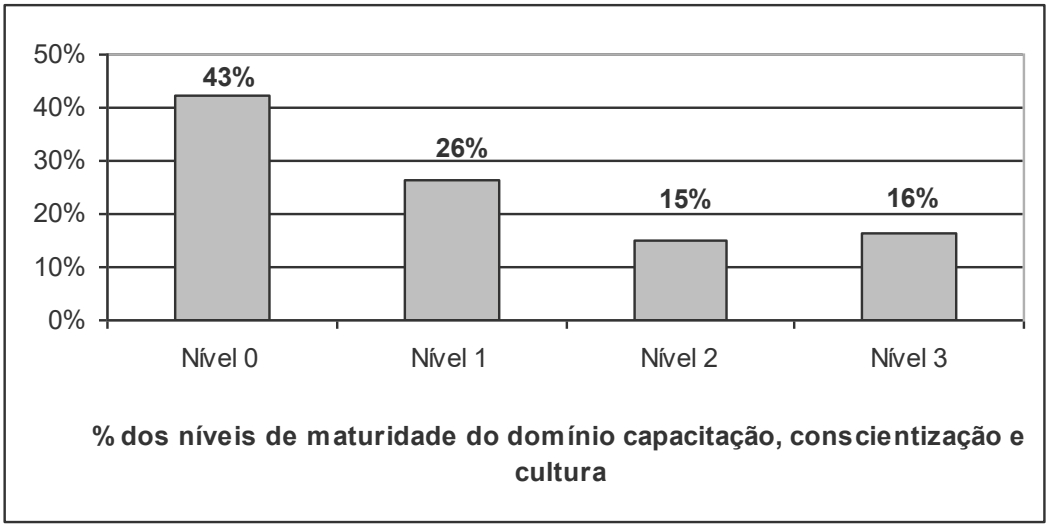



Fonte: elaboração própria.

### 6.2.7 Domínio capacitação, conscientização e cultura

O Gráfico 7 apresenta os percentuais dos níveis de maturidade para este domínio. O elevado percentual para o Nível 0 demonstra a falta de práticas para a criação de uma cultura de SegCiber nas organizações.

**Gráfico 7 | Níveis de maturidade para o domínio capacitação, conscientização e cultura**



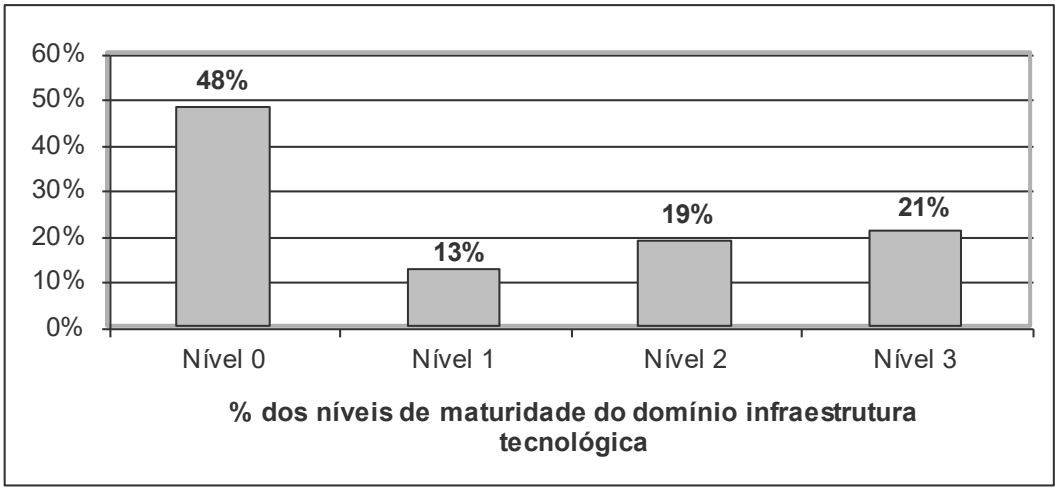

Fonte: elaboração própria.

O treinamento e conscientização da força de trabalho são abordagens tão importantes para a SegCiber quanto as questões tecnológicas. As organizações sem uma cultura de segurança são alvos de engenharia social.[10]

### 6.2.8 Domínio infraestrutura tecnológica

Neste domínio, 48% das organizações estão no Nível 0, ou seja, não têm práticas que definem os requisitos de monitoramento e análise dos eventos de SegCiber. O Gráfico 8 apresenta os percentuais dos Níveis 0, 1, 2 e 3 para o domínio.

**Gráfico 8 | Níveis de maturidade para o domínio infraestrutura tecnológica**

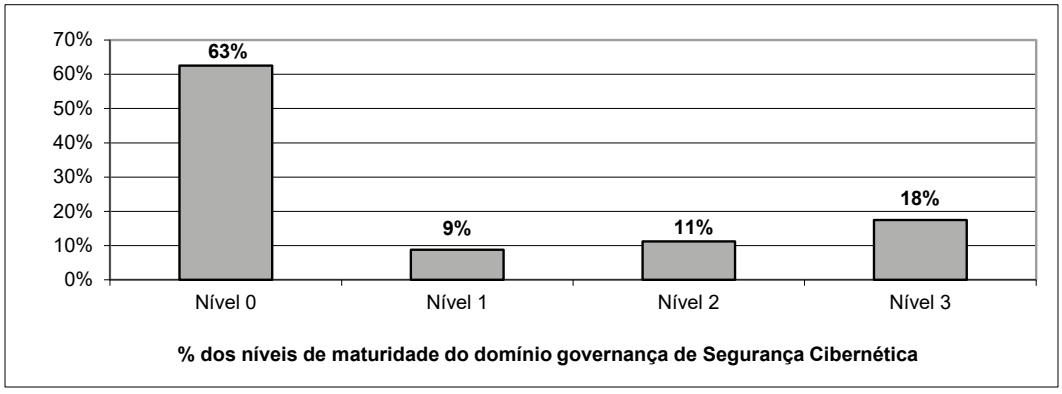



Fonte: elaboração própria.

### 6.2.9 Domínio governança de SegCiber

Os percentuais dos níveis de maturidade para o domínio governança de SegCiber estão apresentados no Gráfico 9. Este é o domínio que tem o maior percentual de organizações no Nível 0 entre todos os domínios. Para o objetivo "patrocinar o programa de SegCiber ", 68,75% das organizações estão no Nível 0, o que significa que as organizações não têm apoio da alta administração para o desenvolvimento e manutenção de políticas de SegCiber.

**Gráfico 9 | Níveis de maturidade para o domínio governança de SegCiber**



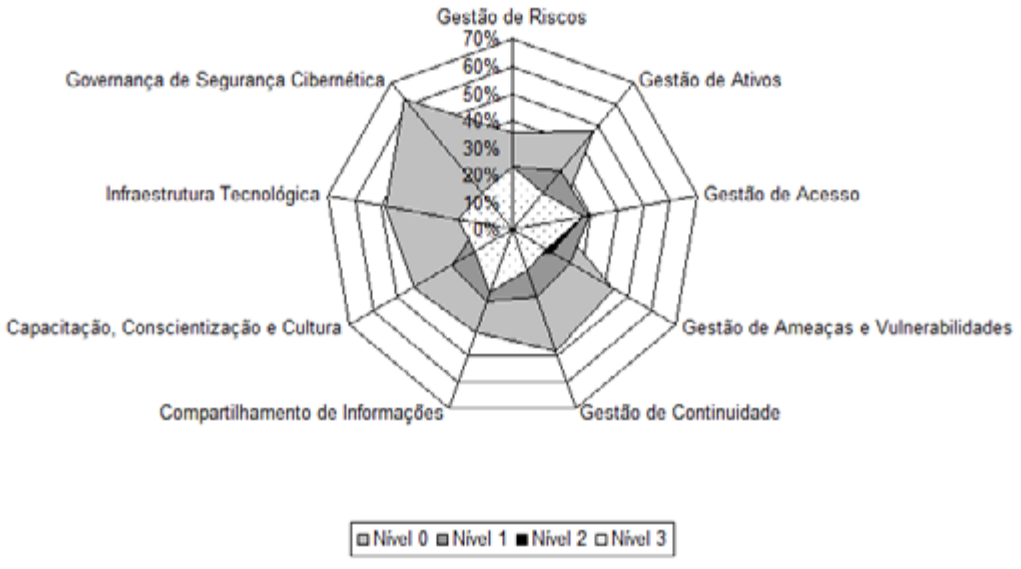

Fonte: elaboração própria.

### 6.2.10 Percentual das organizações por nível

O Gráfico 10 apresenta o percentual das organizações por nível em cada domínio do modelo. Os resultados identificados com a pesquisa demonstram a pouca maturidade de SegCiber entre as organizações participantes deste estudo.

Sendo assim, as organizações da APF não atendem ao objetivo estratégico número VII da Estratégia de Segurança da Informação e Comunicações e Segurança Cibernética do GSI/PR, que estabelece "Elevar o nível de maturidade de SIC e de SegCiber na APF".

**Gráfico 10 – Percentual das organizações por nível**




Fonte: elaboração própria.

## 7 Conclusão

Este estudo propôs o desenvolvimento de um modelo de maturidade de SegCiber cibernética para os órgãos da APF, considerando as similaridades dos temas dos modelos apresentados no referencial teórico e as características da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF.

A estratégia ressalta que não obstante os esforços do governo em fortalecer as ações de SIC e de SegCiber, o que inclui arcabouço de normas complementares publicadas pelo GSI/PR de 2008, o respectivo nível de maturidade ainda está em patamar aquém do desejado nos órgãos da APF (Brasil, 2015).

A referida estratégia estabelece entre suas metas implementar e aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF (Brasil, 2015). No entanto, na pesquisa bibliográfica não foram identificados trabalhos que apresentem os resultados da avalição para elevar a maturidade de SegCiber na APF.

Sendo assim, o levantamento bibliográfico aponta uma reduzida disponibilidade de artigos com a combinação dos termos *Cyber Security* e *Maturity Model*, demonstrando

uma lacuna na literatura sobre o tema. Os artigos encontrados apresentam uma abordagem dos impactos das ameaças e das vulnerabilidades na maturidade de SegCiber das organizações. No estudo dos trabalhos, fica perceptível a necessidade de ações coordenadas por parte das organizações para implementar práticas de compartilhamento de informações referentes à SegCiber, entre elas, estabelecer políticas, diretrizes e normas para proporcionar maior capacidade de resiliência.

Sob o ponto de vista metodológico, foi realizada a análise de conteúdo com a revisão da literatura, a exploração do material, na qual foram organizados os domínios dos modelos selecionados e o tratamento dos resultados para a interpretação dos temas e domínios comuns entre os modelos. A definição dos temas possibilitou o agrupamento de 9 (nove) domínios para o modelo proposto.

Os domínios gestão de riscos, gestão de ativos, gestão de acesso, gestão de ameaças e vulnerabilidades estão alinhados com o objetivo VII da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF. Os domínios gestão de continuidade e infraestrutura tecnológica, por sua vez, estão alinhados com o objetivo IX da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF. O domínio governança de SegCiber está alinhado com os objetivos IV e V da estratégia. Finalmente, os domínios compartilhamento de informações e capacitação, conscientização e cultura estão alinhados com o objetivo III da referida estratégia.

O modelo foi submetido aos gestores de SI de 35 (trinta e cinco) órgãos da APF, por meio de um questionário *online*, para avaliação da maturidade de SegCiber das organizações, atividade prevista na meta XX[11] e XXVI[12] da Estratégia de Segurança da Informação e Comunicações e Segurança Cibernética.

Os resultados da aplicação do modelo mostram que o maior número das organizações pesquisadas está no Nível 0 de maturidade para os domínios definidos para o modelo proposto, conforme os percentuais apresentados na Tabela 1.

[11] Meta XX: implementar e aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF, como mecanismo de acompanhamento e avaliação. Fonte: <http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf>

[12] Meta XXVI: aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF. Fonte: <http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf>

Diante do referido cenário, os resultados obtidos demonstram que há baixa maturidade dos órgãos pesquisados em SegCiber. Os órgãos da APF devem se defender contra a proliferação de ataques cibernéticos e uma defesa efetiva passa pela institucionalização das boas práticas de SegCiber, que fazem parte do modelo proposto.

As contribuições deste trabalho são: a proposta de um modelo de avaliação que permite que as organizações tenham informações sobre o seu nível atual de maturidade de SegCiber e possam implementar melhores práticas de SegCiber; um primeiro olhar sobre a maturidade das organizações da APF em SegCiber; maior visibilidade das práticas de SegCiber implementadas na organização, redesenho de processos de segurança, acompanhamento de indicadores para assegurar a qualidade dos serviços e usuários mais satisfeitos com a segurança na organização.

Os modelos de maturidade C2M2 (2014), *NIST Cybersecurity Framework* (2014) e o CCSMM (2007) que foram apresentados na revisão de literatura não apresentam um alinhamento com a Estratégia de Segurança da Informação e Comunicações e Segurança Cibernética. Sendo assim, a estruturação dos domínios, objetivos e práticas do modelo apresentado visa ao referido alinhamento para atender aos objetivos geral e específicos deste trabalho.

O modelo proposto contribui para o aprimoramento da SegCiber no Brasil. Diante de um contexto de melhorias o modelo terá um ganho de qualidade à medida que for sendo utilizado por um maior número de organizações da APF. O reduzido número de participantes, 35 (trinta e cinco), foi um fator limitante para a pesquisa, além da pouca conscientização das organizações e patrocínio da alta direção nos quesitos afetos à SegCiber, requisitos básicos para implementar as boas práticas de segurança.

Por fim, como trabalhos futuros, sugere-se um levantamento abrangente da maturidade de SegCiber dos órgãos da APF, com orientações sobre melhorias a serem implementadas para alcançar níveis mais elevados de maturidade. Sugere-se, também, o desenvolvimento de uma aplicação *web* e para *smartphone,* como ferramenta para aplicação do modelo, visando aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos da APF.

## Referências bibliográficas


ABNT - NBR ISO/IEC 27032:2015: *Tecnologia da informação - Técnicas de segurança - Diretrizes para segurança cibernética*. Rio de Janeiro: ABNT, 2015.

ABNT – NBR ISO/IEC 27002:2013: *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.* Rio de Janeiro: ABNT, 2013.

ADLER, Richard M. A. *Dynamic capability maturity model for improving cyber security.* Technologies for Homeland Security (HST), IEEE International Conference on. DecisionPath, Inc. Winchester, MA USA. 2013. Disponível em: <http://ieeexplore.ieee.org/document/6699005/?reload=true>. Acesso em: 10 de janeiro de 2017.

AGOSTINI, Marcos Tocchetto. *A cibernética sob a ótica do fenômeno da guerra e da agenda de segurança.* 2014. 92 f. Curso de Relações Internacionais, Centro Socioeconômico, Universidade Federal de Santa Catarina, Florianópolis, 2014.

BARDIN, Laurence. *Análise de conteúdo.* São Paulo: Edições 70, 2011.

_____. *Análise de conteúdo***.** 3ª. reimpressão da 1ª. edição. Título original: L´analyse de contenu. São Paulo: Ed. 70, 2016.

BECKER, J.; KNACKSTEDT, R.; POPPELBUS, J. Developing maturity models for IT management*. Business & Information Systems Engineering*, v.1, n.3, p. 213-222. 2009. Disponível em: <http://dx.doi.org/10.1007/s12599-009-0044-5>. Acesso em: 05 de maio de 2017.

BRASIL. MINISTÉRIO DA DEFESA. 2010. Disponível em:<http://www.defesa.gov.br/>. Acesso em: 30 de abril de 2017.

_____. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da administração pública federal 2015-2018.* Versão 1.0. Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília, 2015. Disponível em: <https://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf >. Acesso em: 25 de novembro de 2016.

_____. TRIBUNAL DE CONTAS DA UNIÃO. *Relatório IgovTI 2014***.** Acórdão nº 3117/2014. Brasília, 2014. Disponível em: <http://www.gestaoti.org/igov/AC_3117_45_14_P.doc>. Acesso em: 05 de abril de 2017.

BRITTO, Tiago Dalpoz*. Levantamento e diagnóstico de maturidade da governança da segurança da informação na administração direta federal brasileira.* Universidade Católica de Brasília. Brasília, 2011. Disponível em: <https://bdtd.ucb.br:8443/jspui/handle/123456789/1331>. Acesso em: 05 de agosto de 2016.

CARVALHO, M. M.; LAURINDO, F. J. B.; PESSÔA, M. S. P*. Information technology project management to achieve efficiency in Brazilian companies.* In: KAMEL, Sherif. (org.). Managing Globally with Information Technology, Hershey, p. 260-271, 2003.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Apostila. Disponível em: <https://books.google.com.br/books?id=oB5x2SChpSEC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 13 de abril de 2017.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5ª ed. São Paulo: Atlas, 2010.

ISACA. Information Systems Audit and Control Association. *Cobit 5.0, modelo corporativo para governança e gestão de TI da organização.* 2012. Disponível em:<http://www.isaca.org/cobit/pages/default.aspx>. Acesso em: 10 de novembro de 2016.

ITGI. *Information security governance:* guidance for information security managers. EUA: ITGI, 2006.

KILLMEYER, Jan. *Information security architecture:* an integrated approach to security in organization. Florida: Auerbach Publications, 2006.

KERZNER, Harold. *Using the project management maturity model:* strategic planning for project management. Kindle Edition. 2006.

MACHADO, Tiago Gerard. *Metodologia de identificação de nível de maturidade de segurança cibernética em smart grid.* Pontifícia Universidade Católica de Campinas. Campinas, 2016. Disponível em: < http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/handle/tede/880>. Acesso em: 15 de janeiro de 2017.

MANDARINO JÚNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro.* Recife, Cubzac, 2010.

MANOEL, Sérgio da Silva. *Governança de segurança da informação*: como criar oportunidades para o seu negócio. Rio de Janeiro, Brasport, 2014.

MUITA, Kevin; MIRON, Walter. *Cybersecurity capability maturity models for providers of critical infrastructure.* Technology Innovation Management Review. 2014. Disponível em:<https://timreview.ca/article/837>. Acesso em: 15 de janeiro de 2017.

NIST. *Framework for improving critical infrastructure cybersecurity. Version 1.0.* Gaithersburg, MD: National Institute of Standards and Technology. 2014. Disponível em: < https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-10?pub_id=915385>. Acesso em: 30 de novembro de 2016.

NUNES, Paulo Fernando Viegas. *A definição de uma estratégia nacional de cibersegurança.* 2012.

OLIVEIRA, Warlei Agnelo. *Modelos de maturidade – visão geral.* Revista Mundo PM. v. 06, dez/jan. 2006. Ano 1. Disponível em: <https://projectdesignmanagement.com.br/produto/revista-06/>. Acesso em: 20 de março de 2017.

PRESIDENTE - The President. *The President of the United States:* executive order 13636 improving critical infrastructure cybersecurity. Federal Register/Presidential Documents, 78(33): February 19, 2013. Washington, DC: U.S. National Archives and Records Administration. Disponível em: <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>. Acesso em: 23 de março de 2017.

PWC. *Pesquisa global de segurança da informação 2016.* Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf>. Acesso em: 13 de abril de 2017.

RAHMAN, H. Amstrong.; MARTI, Jose R.; SRIVASTAVA, K. D. A. *Hybrid systems model to simulate cyber interdependencies between critical infrastructures.* International Journal of Critical Infrastructures,7(4): p.265–288. 2011. Disponível em: <http://dx.doi.org/10.1504/IJCIS.2011.045056>. Acesso em: 10 fevereiro de 2017.

SEI. The Software Engineering Institute. *Capability maturity model® integration (CMMI), version 1.1.* Carnegie Mellon University. 2002. Disponível em: <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14042.pdf>. Acesso em: 23 de novembro de 2017.

SILVA, Elaine M. da. *Cuidado com a engenharia social:* saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais. [S.l.: s. n.], 2008.

SILVA, Sylvio Andre Diogo. *Modelo de capacidade e maturidade para defesa cibernética.* Tese de Mestrado em Informática - Instituto Tecnológico de Aeronáutica. São José dos Campos, 2011. Disponível em: <http://www.bd.bibl.ita.br/tde_busca/arquivo.php?codArquivo=2009>. Acesso em: 25 de janeiro de 2017.

SILVA, Caroline Cordeiro Viana e; PRINS, Ricardo. *Defesa cibernética:* um caminho para securitização? Conjuntura Global, Curitiba, v.2, n. 4, p.230-236, dez. 2013. Quadrimestral.

U.S. Department of Defense. The Software Engineering Institute**.** *Capability maturity model® integration (CMMI), version 1.1.* Carnegie Mellon University. 2002. Disponível em: <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14042.pdf>. Acesso em: 23 de novembro de 2017.

U.S. Department of Energy. *Cybersecurity capability maturity model (C2M2 v1.1).* Department of Energy. Washington, DC: U.S. 2014. Disponível em: <https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf>. Acesso em: 20 de novembro de 2016.

WHITE, Gregory B. *The community cyber security maturity model (CCSMM).* Hawaii International Conference on System Sciences. The Center for Infrastructure Assurance and Security. The University of Texas at San Antonio. 2007. Disponível em: <https://www.researchgate.net/publication/221182620_The_Community_Cyber_Security_Maturity_Model>. Acesso em: 18 de janeiro de 2017.

XIAO-JUAN, Li.; LI-ZHEN, Huang. *Vulnerability and interdependency of critical infrastructure:* a review. Third International Conference on Infrastructure Systems and Services: next Generation Infrastructure Systems for Eco-Cities (INFRA): 1–5. 2010. Disponível em: <http://dx.doi.org/10.1109/INFRA.2010.5679237>. Acesso em: 17 de janeiro de 2017.

**Antonio João Gonçalves de Azambuja**
https://orcid.org/0000-0002-4378-5181

Doutor em Educação e Ciências pela Universidade Federal do Rio Grande do Sul (UFRGS). Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília (UCB). Chefe do Serviço de Segurança da Informação e Comunicações da Advocacia-Geral da União. Certificações: Principles of IT Management (EXIN). Information Security Foundation based on ISO/IEC 27002 (ISFS). EXIN Business Continuity Management Foundation based on ISO 22301 (BCMF). Scrum Fundamentals Certified (SFC). COBIT 5 Foundation.

E-mail: ajaazambuja@gmail.com

**João Souza Neto**
http://orcid.org/0000-0002-4853-8788

Doutor em Engenharia Elétrica pela Universidade de Brasília (Unb). Mestre em Engenharia Eletrônica pelo Philips International Institute da Holanda. Professor do Mestrado em Governança, Tecnologia e Inovação da Universidade Católica de Brasília. É certificado CGEIT, CRISC Trainer, CDSPE, COBIT 2019 Trainer, COBIT 2019 Design & Implementation, COBIT 5 Trainer, COBIT Certified Assessor, PMP, RMP, RCDD. É IEEE Senior Member. Presidente e membro fundador do Capítulo Brasília da ISACA.

E-mail: sznetoj@gmail.com