Modelo de maturidade de segurança cibernética para os órgãos da Administração Pública Federal

Antonio João Gonçalves de Azambuja[1], João Souza Neto[2]

[1] Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília (UCB). Doutorando da Universidade Federal do Rio Grande do Sul (UFRGS). Chefe do Serviço de Segurança da Informação e Comunicações da Advocacia-Geral da União (AGU).
[2] Doutor em Engenharia Elétrica pela Universidade de Brasília (UnB), Professor do Mestrado de Governança, Tecnologia e Inovação da Universidade Católica de Brasília (UCB).

{ajaazambuja@gmail.com, sznetoj@gmail.com}

Abstract. *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 as technical procedures. 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 to some agencies of the Brazilian Federal Public Administration. The results evidenced that, in general, the agencies surveyed have low maturity in Cybersecurity.*

Resumo. *O artigo apresenta um modelo de maturidade de Segurança Cibernética (SegCiber) para os órgãos da Administração Pública Federal (APF). Foi realizada uma pesquisa qualitativa para analisar os modelos de maturidade de SegCiber encontrados na literatura, que foram a 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, que permitiu a definição dos domínios do modelo proposto. Os resultados da aplicação do modelo, por meio do questionário online, demonstram que, no geral, há baixa maturidade dos órgãos pesquisados.*

1. Introdução

A informação tem se mostrado, nos dias atuais, 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).

A Estratégia de Segurança da Informação e Comunicações e de Segurança

Cibernética da Administração Pública Federal (BRASIL, 2015) define a Segurança Cibernética (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.

Para a norma ABNT NBR ISO/IEC 27032:2015, as práticas básicas de Segurança da Informação (SI) voltadas para as partes interessadas no espaço cibernético fornecem as diretrizes para melhorar o estado de SegCiber, determinando os aspectos comuns dessa atividade e suas ramificações em outros domínios de segurança, tais como: as redes computadores e a proteção de infraestruturas críticas de informação (ABNT, 2015).

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

O espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, desafiando conceitos tradicionais, entre eles, o de fronteiras geopolíticas e organizacionais, constituindo novo território, por vezes desconhecido, a ser desbravado pelos bandeirantes do século XXI (Machado, 2010).

A avaliação da 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.

Do ponto de vista da SegCiber, deve-se adotar ações que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações de interesse do Estado brasileiro (Mandarino Júnior, 2010), os quais são princípios básicos da SI.

Entre as metas descritas na atual Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, 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, este artigo busca apresentar um modelo de maturidade de SegCiber para ajudar as organizações públicas a avaliarem o seu estado atual da SegCiber e assegurar a continuidade do negócio. Para tal, apresenta um referencial teórico, metodologia utilizada na pesquisa e os resultados da aplicação do modelo com a participação de 35 organizações.

2. Referencial Teórico

2.1. Estratégia de Segurança da Informação e Comunicações e SegCiber da APF

A Estratégia é um instrumento de apoio ao planejamento estratégico governamental que reúne um conjunto de objetivos estratégicos e metas para o período de 2015 a 2018, elaborada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Considerando que são atividades estratégicas 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 SIC e de SegCiber, o que inclui o arcabouço de normas complementares publicadas pelo GSI desde 2008, no geral, os níveis de maturidade dos órgãos da APF ainda se encontram em patamar aquém do desejado (BRASIL, 2015).

2.2. Norma ISO/IEC 27032:2012

A Norma ISO/IEC 27032:2012 estabelece diretrizes para melhorar o estado de SegCiber de uma organização, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.

Aborda a SegCiber como 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, que não existe em nenhum formato físico (ABNT, 2015).

2.3. Modelos de maturidade de SegCiber

2.3.1. *Cybersecurity Capability Maturity Model* (C2M2)

O *Cybersecurity Capability Maturity Model* (U.S. Department of Energy, 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 e gestão de SegCiber associadas aos ativos de TI, operações de tecnologia e o seu ambiente de operação.

As organizações podem usar esse documento para os seguintes fins: **i)** fortalecer as capacidades de SegCiber; **ii)** permitir a avaliação de forma eficaz e consistente do estado atual da SegCiber; **iii)** compartilhar conhecimento, melhores práticas e referências de SegCiber; e **iv)** permitir a priorização das ações e investimentos para melhorar a SegCiber.

O modelo apresenta uma metodologia de autoavaliação nas organizações, visando a 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; gestores responsáveis pela gestão de recursos e operações organizacionais; gestores responsáveis pela aplicação da autoavaliação; e facilitadores da aplicação de autoavaliação.

O C2M2 usa uma escala de quatro níveis, que permite à organização definir o seu estado atual de SegCiber, determinar o futuro desejado e identificar os recursos necessários para alcançar esse estado futuro.

2.3.2. *NIST Cybersecurity Framework*

O modelo foi desenvolvido em resposta a uma ordem 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 encoraje a eficiência, inovação e prosperidade econômica (The President, 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. Tem as seguintes funções e objetivos: **i)** identificar:

desenvolver a compreensão organizacional para gerenciar o risco de sistemas, ativos, dados e recursos; **ii)** proteger: desenvolver e implementar as salvaguardas adequadas para assegurar os serviços de infraestrutura crítica; **iii)** detectar: desenvolver e implementar as atividades apropriadas para identificar a ocorrência de eventos de SegCiber; **iv)** responder: desenvolver e implementar as atividades apropriadas para tomar medidas relativas a eventos de SegCiber detectados; e **v)** recuperar: desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido a eventos de SegCiber.

Os níveis utilizados no modelo são: **i)** parcial; **ii)** informado; **iii)** repetido; e **iv)** adaptado. Esses níveis descrevem um grau crescente de rigor e sofisticação nas práticas de risco de SegCiber e a sua integração com o risco global da organização e as suas necessidades para o negócio.

2.3.3. *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.

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.

3. 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 a análise de conteúdo e um questionário *online*.

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).

A análise de conteúdo, por sua vez, representa um conjunto de técnicas de análise de comunicações que visam a 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 ou recepção (variáveis inferidas) destas mensagens (Bardin, 2011).

A análise de conteúdo, conforme Bardin (2011), prevê 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.

3.1 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.

3.2 Análise de conteúdo

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

3.2.1 Pré-análise

As atividades realizadas foram:

- Revisão da literatura;
- Organização do material; e
- Relacionamentos dos pontos relevantes e comuns entre os modelos.

3.2.2 Tratamento dos resultados

A definição dos temas permitiu o agrupamento em nove domínios, para o modelo proposto, conforme 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.

4. Apresentação dos resultados

Os resultados obtidos com a pesquisa possibilitaram a elaboração do Modelo de Maturidade de SegCiber para os órgãos da APF, com nove domínios, 33 objetivos, 56 práticas para o Nível 1 (N-1), 111 práticas para o Nível 2(N-2) e 117 práticas para o Nível 3 (N-3).

4.1 Níveis de maturidade para o modelo proposto

Os níveis são utilizados para medir a competência organizacional ou maturidade de um conjunto reconhecido das melhores práticas. No quadro 1 são apresentados os domínios do modelo proposto e o seu relacionamento com domínios dos modelos estudados. O modelo do C2M2 contribuiu com dez domínios, o modelo do NIST com três e o modelo elaborado por White (2007) com seis.

Quadro 1 - 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
1. Gestão de risco	·	·	
2. Gestão de ativos	·		
3. Gestão de acesso	·		
4. Gestão de ameaças e vulnerabilidades	·		·
5. Gestão de continuidade	·		
6. Compartilhamento de informações	·	·	·
7. Capacitação, conscientização e cultura	·	·	·
8. Infraestrutura tecnológica	·		·
9. Governança de SegCiber	·		
Total de domínios dos modelos	10	3	6
Percentual dos relacionamentos dos domínios com os modelos	47,36% (9)	15,78% (3)	21,05% (4)

Fonte: Os autores

No quadro 1, é possível identificar que o maior percentual de alinhamento dos domínios do modelo proposto ocorre com os domínios do C2M2, com um percentual de 47,36 %, contra 15,78% para o modelo do NIST e 21,05% para o modelo CCSMM.

A justificativa para selecionar os domínios do modelo C2M2 foi o maior percentual de alinhamento entre os domínios do modelo proposto e os domínios do C2M2, conforme apresentado no quadro 1.

4.2 Domínios do modelo de maturidade proposto

Cada um dos 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.

O modelo proposto fornece uma orientação para ajudar as organizações medir e melhorar as suas capacidades de SegCiber com base nos padrões existentes.

4.2.1 Segue uma breve descrição dos domínios do modelo:

- Gestão de riscos: a gestão de riscos em SegCiber fornece orientação para analisar e priorizar o risco e define a tolerância ao risco;
- Gestão de ativos: realizar 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: a 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: a 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: a 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: visa estabelecer e manter relações com entidades internas e externas para coletar e compartilhar informações sobre SegCiber;
- Capacitação, conscientização e cultura: procura criar uma cultura de SegCiber na organização e assegurar a adequação das competências atualizadas para a força de trabalho;
- Infraestrutura tecnológica: requer uma infraestrutura tecnológica com mecanismos para identificar, tratar e responder as ameaças e vulnerabilidades de forma integrada; e
- Governança de SegCiber: visa estabelecer e manter um programa corporativo de SegCiber que forneça governança, planejamento estratégico e patrocínio para as atividades de SegCiber.

4.3 Estrutura do modelo proposto

As práticas para cada um dos domínios estão agrupadas por objetivos que apoiam a estrutura do modelo. Na tabela 1 estão apresentados os nove domínios, trinta e três objetivos e o número de 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 risco	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

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 SegCiber				
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: Os autores

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

Para aplicação do modelo, a organização deve selecionar um avaliador que esteja familiarizado com a estrutura do modelo e tenha, também, conhecimento para ajudar a organização a entender os seus objetivos e realizar um planejamento para atingir níveis mais elevados de maturidade.

4.4 Resultados da aplicação do modelo

Para aplicação do modelo, foram selecionadas 35 (trinta e cinco) organizações da APF, que relataram a necessidade de assegurar a confidencialidade, integridade e disponibilidade das suas informações, garantindo a proteção dos seus ativos de informação e das suas infraestruturas críticas para continuidade do negócio.

A tabela 2 apresenta o percentual das organizações por nível para cada um dos objetivos dos domínios do modelo proposto.

Tabela 2 - Percentuais dos objetivos

Domínios	Percentuais			
	Nível 0	Nível 1	Nível 2	Nível 3
Gestão de Risco)	34,38	26,56	18,75	20,31
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
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	46,88	28,13	7,81	17,19
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	47,92	27,08	8,33	16,67
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	43,75	25,00	16,67	14,58
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	47,50	26,25	10,00	16,25
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
Responder a incidentes e eventos escalados de SegCiber	37,50	37,50	12,50	12,50
Domínios	Percentuais			
	Nível 0	Nível 1	Nível 2	Nível 3
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	40,63	28,13	6,25	25,00
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	42,50	26,25	15,00	16,25
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	47,92	12,50	18,75	20,83
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 SegCiber	62,50	8,75	11,25	17,50
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: Os autores

Para domínio gestão de riscos, 34,38 % das organizações estão no N-0, ou seja, não realizam práticas de gestão de riscos. O elevado número de organizações no N-0 demonstra a falta de uma estratégia de gestão de riscos de SegCiber.

No domínio gestão de ativos, o percentual de organizações no N-0 foi de 46,88%, maior que no domínio gestão de riscos. Com a falta de maturidade nesse 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.

Os resultados do domínio gestão de acesso apresentam o menor percentual de organizações no N-0 em comparação com os demais. O fato da maioria das organizações estar no N-1, N-2 e N-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.

No domínio gestão de ameaças e vulnerabilidades a maior parte das organizações pesquisadas está no N-0 para esse 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.

Os níveis de maturidade das organizações para o domínio gestão de continuidade apresentaram os seguintes percentuais: 47,50 % (N-0), 26,25 % (N-1), 10 % para o (N-2) e 16,25 % (N-3). A baixa maturidade para esse domínio demonstra que as organizações não possuem planos, procedimentos e tecnologias para sustentar as operações das organizações como resposta a eventos de SegCiber.

O maior número das organizações está no N-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).

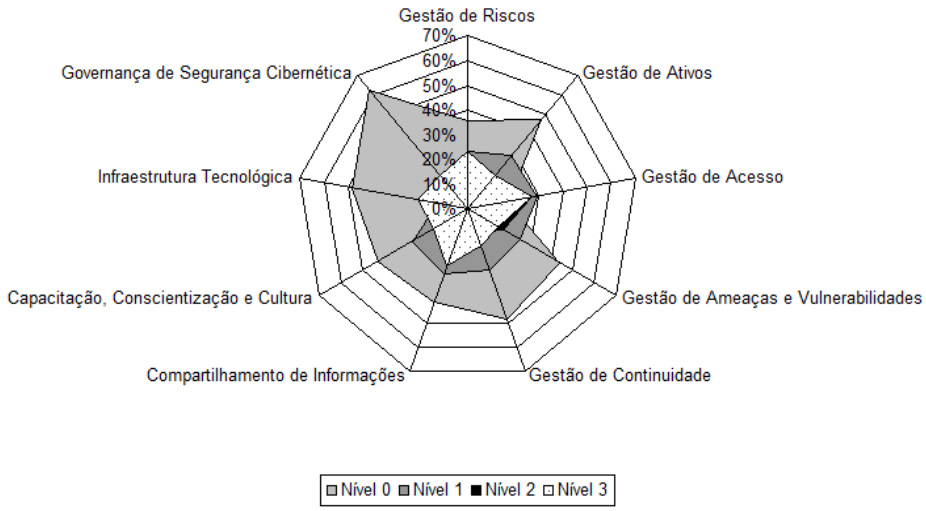
Para o para o domínio capacitação, conscientização e cultura existe um elevado percentual das organizações no N-0. Tal resultado demonstra a falta de práticas para a criação de uma cultura de SegCiber nas organizações. O treinamento e conscientização da força de trabalho são abordagens tão importantes para a SegCiber quanto as questões tecnológicas.

O domínio infraestrutura tecnológica tem um percentual de 47,92 % das organizações no N-0, ou seja, não têm práticas que definem os requisitos de monitoramento e análise dos eventos de SegCiber.

Os percentuais dos níveis de maturidade para o domínio governança de SegCiber demonstram que a maioria das organizações está no N-0 entre todos os domínios. Para o objetivo "patrocinar o programa de SegCiber", 68,75% das organizações estão no N-0, o que significa que as organizações não têm apoio da alta administração para o desenvolvimento e manutenção de políticas de SegCiber.

O Gráfico 1 apresenta o percentual das organizações por nível em cada domínio do modelo.

Gráfico 1 - Percentual das organizações por nível



Fonte: Os autores

5. Conclusão

Este estudo propôs o desenvolvimento de um modelo de maturidade de SegCiber para os órgãos da APF, considerando as características dos modelos apresentados no referencial teórico e as características da Estratégia de SIC e de SegCiber da APF.

Assim sendo, foi realizada a análise de conteúdo com a fase de pré-análise, que foi a revisão da literatura, a fase de exploração do material, na qual foram organizados os domínios dos modelos selecionados e a fase de tratamento dos resultados para a interpretação dos temas e domínios comuns entre os modelos. A definição dos temas possibilitou o agrupamento de nove domínios para o modelo proposto.

O modelo foi submetido aos órgãos participantes por meio de questionário *online*, para uma avaliação da maturidade de SegCiber das organizações, atividade prevista na meta XXI e XXII da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF.

Com a aplicação do modelo foi possível identificar, entre as organizações participantes que, no geral, há baixa maturidade dos órgãos pesquisados em SegCiber. Os resultados demandam ações de melhoria por parte das organizações que possuem ativos de informação que devem ser protegidos de ameaças cibernética.

O maior número das organizações está no Nível 0 (N-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 Segurança da Informação e Comunicações e Segurança Cibernética na APF.

As organizações da APF devem planejar ações que fortaleçam a defesa nacional para mitigar vulnerabilidades que podem ser exploradas com os avanços tecnológicos no espaço cibernético e o crescimento das interações entre os usuários e a tecnologia, visando a continuidade do negócio na era da sociedade da informação.

Referências

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.

ABNT - NBR ISO/IEC 27032:2012: Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética. Rio de Janeiro: ABNT, 2015.

Bardin, l. Análise de conteúdo. São Paulo: Edições 70, 2011.

Brasil. Desafios estratégicos para segurança e defesa cibernética. Secretaria de Assuntos Estratégicos da Presidência da República. Organizadores: Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. Brasília, 2011. Disponível em: <http://www.biblioteca.presidencia.gov.br/presidencia/dilma-vana-rousseff/publicacoes/orgao-essenciais/secretaria-de-assuntos-estrategicos/deafios-estrategicos-para-a-seguranca-e-defesa-cibernetica/view>. Acesso em: 05 de abril de 2017.

Brasil. 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/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 25 de novembro de 2016.

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.

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://www.bdtd.ucb.br/tede/tde_busca/arquivo.php?codArquivo=1429>. 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.

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/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. Acesso em: 30 de novembro de 2016.

Rahman, H. A.; Marti, J. R.; Srivastava, K. D. A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures*,7(4): 265–288. 2011. Disponível em: <http://dx.doi.org/10.1504/IJCIS.2011.045056>. Acesso em 10 fevereiro de 2017.

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.

U.S. Department of Defense. The Software Engineering Institute. Capability Maturity Model® Integration (CMMI), Version 1.1. Carnegie Mellon University. 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.computer.org/csdl/proceedings/hicss/2007/2755/00/27550099b.pdf>. Acesso em: 18 de janeiro de 2017.

Xiao-Juan, l.; Li-Zhen, H. 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 janeiro de 2017.