Proposta de avaliação da Política Nacional de Segurança da Informação por Processo de Análise Hierárquica

Clarice Saraiva Andrade dos Santos [I]
https://orcid.org/0000-0002-3500-7347

Luiz Octávio Gavião [II]
https://orcid.org/0000-0002-3580-7085

Leonardo Augusto dos Santos Oliveira [III]
https://orcid.org/0000-0001-6515-6346

José Cristiano Pereira [IV]
https://orcid.org/0000-0002-2329-0560

[I] *Escola Superior de Guerra, RJ, Brasil.*
Mestre em Segurança Internacional e Defesa pela Escola Superior de Guerra.

[II] *Escola Superior de Guerra, RJ, Brasil.*
Doutor em Engenharia de Produção na Universidade Federal Fluminense. Professor Adjunto na Escola Superior de Guerra.

[III] *Escola Superior de Guerra, RJ, Brasil.*
Doutor em Administração de Empresas na Fundação Getúlio Vargas. Professor Adjunto na Escola Superior de Guerra.

[IV] *Universidade Católica de Petrópolis, RJ, Brasil.*
Pós-doutorando no Laboratório Nacional de Computação Científica.

http://dx.doi.org/10.1590/1981-5344/29373

Relatórios recentes de segurança cibernética evidenciam que o Brasil é um dos países com a maior quantidade de crimes cibernéticos, afetando mais de 60 milhões de pessoas e causando prejuízos estimados em mais de 20 bilhões de dólares. No âmbito da Administração Pública

Federal, a Política Nacional de Segurança da Informação (PNSI) atribuiu ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a tarefa de monitorar e avaliar a sua execução, estimulando a ampla participação da sociedade e dos órgãos e das entidades do Poder Público na construção do processo, o que inclui a academia. A fim de contribuir com esse contexto, esta pesquisa analisou diferentes modelos de referência, cuja estrutura melhor se ajustasse à necessidade de avaliar instituições e um método quantitativo capaz de indicar objetivamente o peso das diversas variáveis envolvidas. O modelo de maturidade escolhido foi o CSF-NIST e o método selecionado foi o Processo de Análise Hierárquica (AHP), para a ponderação dos critérios e subcritérios. Um estudo de caso foi explorado para ilustrar a aplicação do modelo e do método selecionados, indicando o "como" implementá-los, considerando as especificidades da instituição avaliada.

Palavras-chave: *Segurança da Informação. Modelos de Maturidade. Processo de Análise Hierárquica.*

Evaluation of the national information security policy by analytic hierarchy process

Recent cybersecurity reports show that Brazil is one of the countries with the highest number of cybercrimes, affecting more than 60 million people and causing losses estimated at more than 20 billion dollars. Within the scope of the Public Administration, the National Information Security Policy (PNSI) assigned to the Institutional Security Office of the Presidency (GSI/PR) the task of monitoring and evaluating its execution, stimulating the broad participation of society and agencies and public authorities in the construction of the process, which includes the academic effort. To contribute to this context, this research analyzed different reference

models, whose structure best suited the needs of the institutions evaluated and a quantitative method capable of objectively indicating the weight of the various variables in the model. The maturity model chosen was the CSF-NIST and the method selected was the Analytic Hierarchy Process (AHP), for weighting the criteria and sub criteria. A case study illustrates the application of the selected model and method, indicating "*how*" to implement them, considering the specificities of the evaluated institution.

Keywords: *Information Security. Maturity Models. Analytic Hierarchy Process.*

Recebido em 07.02.2021 Aceito em 21.12.2022

1 Introdução

Na "era da informação", caracterizada por avanços tecnológicos em sistemas informatizados e transmissão de significativo volume de dados em redes, revolucionou-se a maneira através da qual as sociedades se comunicam. A velocidade e o volume de dados informatizadas trouxeram impactos na economia, na política e para a segurança nacional e internacional (CAVELTY; BRUNNER, 2007a). Entretanto, esse desenvolvimento tecnológico foi acompanhado de novos riscos e prejuízos financeiros. De acordo com um relatório da empresa Symantec, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões, atrás apenas da China, que teve um prejuízo de US$ 66,3 bilhões. Um dos principais fatores deste aumento de crimes está na popularidade de *smartphones*, cuja quantidade de aparelhos no país supera a marca de 230 milhões de unidades, maior que a própria população do país (SYMANTEC, 2018).

Em 2018, o Grupo de Resposta a Incidentes de Segurança para a internet no Brasil, do Comitê Gestor da Internet, responsável por registrar os incidentes de segurança em computadores de redes conectadas à internet no país, recebeu o reporte de 678.514 incidentes. O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR-Gov) recebeu o reporte de 20.522 incidentes, sendo 9.981 incidentes

confirmados em 2018, apenas no âmbito da Administração Pública Federal (BRASIL, 2020b).

Diante desses desafios, instituições públicas e privadas precisaram regular as atividades de segurança através de políticas, visando orientar os procedimentos referentes à segurança cibernética[1]. Diversos países têm suas políticas e estratégias relacionadas à segurança cibernética publicadas de forma ostensiva. De igual forma, o meio acadêmico também tem acompanhado as discussões nacionais e internacionais acerca do tema, tanto no aspecto da elaboração de políticas quanto na criação de medidas de natureza cibernética que ampliem a segurança das instituições e das sociedades, em última análise (CAVELTY; BRUNNER, 2007b; GOIS, 2018; LIMA, 2018; VIANNA; DE SOUSA, 2018).

No âmbito do governo brasileiro, o problema da segurança dos dados e sistemas foi inicialmente abordado através do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), em 2001, ao ser designado para a coordenação das atividades de segurança da informação. Em 2008, o Departamento de Segurança da Informação e Comunicação (DSIC), vinculado ao GSI/PR, foi criado com a tarefa de planejar e coordenar a execução de atividades de segurança da informação e comunicação na área da administração pública federal.

Recentemente, o Congresso Nacional aprovou o Decreto Nº 9.637, em 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação (PNSI), com a finalidade de orientar a governança da segurança da informação, abrangendo: "I - a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação". Nesse Decreto também inclui-se o incentivo à pesquisa acadêmica nos objetivos do Artigo 4º, que destaca o fomento às atividades de pesquisa científica, de desenvolvimento tecnológico e de

1 De fato, a expressão "segurança cibernética" recebe diferentes definições. Por exemplo, a União Internacional das Comunicações (órgão da ONU) define "segurança cibernética" como "a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e propriedades de usuários(as). A organização e as propriedades incluem dispositivos de computação conectados, funcionários(as) e colaboradores(as), infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético. A segurança cibernética busca garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético" (ITU-CIBERSEG, 2008). No Brasil, o Gabinete de Segurança Institucional da Presidência da República define "segurança cibernética" como "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2015).

inovação relacionadas à segurança da informação. Esses aspectos indicam que a PNSI pode ser aperfeiçoada a partir de sugestões que contribuam ao desenvolvimento da atividade de segurança da informação e, dessa forma, motivaram a realização desta pesquisa. No parágrafo único do Artigo 6º, o Decreto descreve que a "*construção da Estratégia Nacional de Segurança da Informação terá a ampla participação da sociedade e dos órgãos e das entidades do Poder Público*"; no item VII do Artigo 12º, o Decreto descreve que o GSI-PR deve "*estabelecer critérios que permitam o monitoramento e a avaliação da execução da PNSI e de seus instrumentos*". Assim, uma proposta de uma estrutura ponderada de critérios e subcritérios para avaliar a execução da PNSI, com a participação técnica de especialistas em segurança da informação, constitui o foco desta pesquisa (BRASIL, 2018).

Uma proposta de critérios para a avaliação da PNSI é uma tarefa complexa, considerando a variedade de grupos de interesse que integram a comunidade de segurança da informação, nas mais diferentes esferas do poder público e privado. A multidisciplinaridade do CGSI, envolvendo representantes de todos os Ministérios e diversos órgãos públicos, evidencia a amplitude e capilaridade do tema na sociedade. Além disso, a atividade de segurança da informação gera diferentes experiências às instituições envolvidas, no país e no exterior.

Assim, esta pesquisa levantou e adaptou critérios utilizados em modelos de maturidade consagrados na prática de identificação e gerenciamento de riscos cibernéticos em infraestruturas críticas. A interrupção de serviços essenciais decorrentes de infraestruturas críticas é considerada de sério impacto, por suas consequências sociais, econômicas, políticas, ambientais, capazes de pôr em risco a segurança do Estado (BRASIL, 2018). Para lidar com este problema complexo, se torna fundamental a habilidade de mensurar quantitativamente as performances destes critérios nas organizações. Para tanto, o uso de metodologia de apoio à decisão multicritério favorece a compreensão dos elementos do modelo conceitual através de uma pontuação de relevância.

O Decreto Nº 9.637 é ainda recente para que as medidas necessárias sejam plenamente implementadas e apresentem efeito útil e prático dessa política para a sociedade. Desta forma, qualquer proposta de aprimoramento de políticas públicas relacionadas à segurança da informação traz significativa utilidade para a sociedade, em função dos prejuízos que a proposta pode evitar ao proteger dados e informações estratégicas ao país, às suas instituições e ao seu patrimônio público e privado. As instâncias de perdas e danos referentes à segurança e defesa cibernética são marcantes e justificam os esforços e recursos priorizados em suas atividades. Por efeito colateral, a "era da informação" também beneficiou invasores de sistemas, os chamados *hackers*, que tanto

prejuízo causam a sistemas públicos e privados (BUCHANAN, 2020; STERLING, 2020; WHITE, 2020).

O tema ainda é atual e relevante para a defesa nacional, posto que a segurança e as respostas às ameaças em rede, em consequência dos avanços na tecnologia da informação e das comunicações, integram capacidades fundamentais para a construção de uma Defesa Nacional forte. Em 2010, a expressão "segurança cibernética" foi oficialmente publicada no Livro Verde, pela Presidência da República (BRASIL, 2010). O setor cibernético, juntamente com o nuclear e aeroespacial, foi elencado na Estratégia Nacional de Defesa (END) com relevância estratégica ao país, em função da necessidade de aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos (BRASIL, 2020a; NETO, 2020; RAMOS; GOLDONI, 2016).

Para a comunidade acadêmica, pretende-se incitar a discussão sobre os aspectos mais técnicos necessários para implementar políticas públicas e acompanhar a matéria de segurança cibernética, que representa uma tendência mundial. O estudo tangencia a preocupação expressa pelo Estado brasileiro na fundação de um arcabouço essencial para tratar a proteção de seus dados e a manutenção da segurança no ambiente cibernético. Verifica-se, deste modo, que esta pesquisa traz relevância ao tema, por contribuir com o governo brasileiro a obter êxito no atingimento dos objetivos da PNSI, através da identificação de uma estrutura de apoio à decisão e formas de avaliação para a implementação de uma Estratégia Nacional de Segurança da Informação (ENSI).

2 Delineamento da pesquisa

Um problema de pesquisa foi estruturado, conforme o Quadro 1, para identificar que estrutura hierárquica e ponderada de critérios e subcritérios permite auxiliar no monitoramento e a avaliação da execução da PNSI e de seus instrumentos nos diferentes campos de atuação. Esta questão se origina no próprio Decreto Nº 9.637, que através do Artigo 12º, item VII, determina o estabelecimento de "*critérios que permitam o monitoramento e a avaliação da execução da PNSI e de seus instrumentos*" (BRASIL, 2018).

A "estrutura hierárquica" aqui proposta se refere à necessidade de agrupar conjuntos de critérios e eventuais subcritérios em diferentes níveis de especificidade técnica. Esse tipo de estrutura permite que um problema seja descrito em diferentes níveis, reduzindo a sua complexidade em termos de análise e de compreensão dos seus usuários. Isto é relevante pois o Decreto Nº 9.637 não limita o monitoramento e avaliação a um determinado órgão da administração pública, cabendo a

cada Instituição o exercício dessas atividades. Nesse contexto, a compreensão dos usuários é essencial.

A "estrutura ponderada" indica a possibilidade de propor critérios e subcritérios com importância relativa, permitindo avaliar uma política com maior peso em um conjunto de critérios e menores pesos em outros. Isto confere maior realismo à proposta, pois permite que o processo atribua maior importância aos aspectos mais relevantes ao decisor. Além disso, o domínio da metodologia aqui proposta permite que cada diferente órgão construa a sua própria estrutura de pesos, partindo dos critérios básicos da estrutura hierárquica.

A menção aos "diferentes campos de atuação" se refere à necessidade de envolver os mais diversos grupos de interesse na pesquisa, de forma que a estrutura proposta possa servir a diferentes órgãos e instituições públicas ou privadas que aplicam as diretrizes da PNSI, ou mesmo que possam utilizá-la como modelo de referência para adaptar suas estruturas de segurança da informação e cibernética.

Quadro 1 – Etapas e procedimentos da pesquisa

PROBLEMA DE PESQUISA			
Que estrutura hierárquica e ponderada de critérios e subcritérios permite auxiliar no monitoramento e a avaliação da execução da PNSI e de seus instrumentos nos diferentes campos de atuação?			
Questões da pesquisa	Objetivos específicos	Etapas / Resultados Parciais	Localização neste Artigo
Que modelo conceitual e que método quantitativo de monitoramento e avaliação de sistemas de segurança da informação e cibernética devem ser utilizados para atender às necessidades estabelecidas pelo Decreto No 9.637?	Levantar e selecionar, com base na literatura científica, modelos conceituais de referência ao monitoramento e avaliação de sistemas de segurança da informação e cibernética;	1. Levantamento da literatura para a busca de modelos dos conceituais;	Seção 3, Quadro 2
		2. Seleção do modelo conceitual para a aplicação na pesquisa	Subseção 3.1
	Levantar e selecionar, com base na literatura científica, metodologia quantitativa de Pesquisa Operacional capaz de ponderar critérios de monitoramento e avaliação das políticas públicas relacionadas à segurança da informação e cibernética;	3. Levantamento da literatura para a busca de modelos da Pesquisa Operacional	Subseção 4.1
		4. Seleção do modelo de Pesquisa Operacional para a aplicação na pesquisa	Subseção 4.1
Como obter os pesos dos critérios e subcritérios do modelo escolhido para monitorar e avaliar uma Instituição pública ou privada?	Ponderar os critérios escolhidos com base na metodologia de Pesquisa Operacional selecionada;	5. Elaboração da estrutura hierárquica do problema	Seção 5
		6. Elaboração dos questionários de avaliação	Subseção 5.1
		7. Coleta dos dados aos estudos de caso	Subseção 5.1
		8. Cálculo dos pesos dos critérios e subcritérios	Subseção 5.1
		9. Cálculo das Razões de Consistência para a validação do modelo	Subseção 5.1
	Aplicar experimentalmente o modelo referência e o método quantitativo selecionado em estudo de caso.	10. Análise dos resultados da aplicação	Subseção 5.2

Fonte: autoria própria

A Etapa 1 efetuou o levantamento da literatura para a busca de modelos dos conceituais de monitoramento e avaliação de sistemas de segurança da informação e cibernética. Inicialmente foram levantados 13 modelos: CMM, CMMI, ISO/IEC 27000, COBIT5, ISA/IEC 62443 (ISA-99), CIS-CSC, ISM2, ISM3, C2M2, CSF, IAMM, CAF e NCSG. Esses modelos foram descritos e analisados, sendo delimitados a uma lista de quatro modelos de referência para uma análise mais aprofundada: CSF, CAF, NCSG e o ISO/IEC 27000. Posteriormente, na Etapa 2, o CSF do NIST foi o modelo selecionado para o prosseguimento da pesquisa.

Na Etapa 3, buscou-se na literatura científica por métodos da Pesquisa Operacional capazes de solucionar o problema. Na maioria dos casos encontrados, o AHP foi o modelo quantitativo explorado para a avaliação de políticas públicas. O AHP é um método quantitativo amplamente explorado em Pesquisa Operacional para o estabelecimento de pesos em problemas de apoio à decisão (POMEROL; BARBA-ROMERO, 2012). Dessa forma, na Etapa 4 confirmou-se o modelo, com base nos principais artigos encontrados.

A Etapa 5 consistiu na transposição da estrutura do CSF-NIST em uma hierarquia. Uma vez que o modelo está estruturado em funções objetivas, sua disposição já se encontra disposta em níveis e subníveis para a aplicação do modelo quantitativo.

As Etapas 6 a 9 reúnem procedimentos de cálculo inerentes ao método AHP. Após a seleção do modelo de maturidade e organização da estrutura hierárquica de critérios e subcritérios, a pesquisa prosseguiu com a elaboração dos questionários de avaliação, a coleta dos dados ao estudo de caso, o cálculo dos pesos dos critérios e subcritérios e o cálculo das Razões de Consistência para a validação do modelo.

Na Etapa 10, os resultados obtidos no estudo de caso foram analisados.

3 Modelos de avaliação e monitoramento de sistemas

A identificação dos modelos mais bem estruturados para avaliar essas políticas é uma tarefa complexa, em vista das diferentes abordagens e propósitos da avaliação. Por este motivo, é necessário recorrer a bases de dados e de publicações científicas para levantar os modelos de monitoramento e avaliação mais explorados, que sirvam de referência para a análise nesta pesquisa. Por vezes, os modelos são designados através de diferentes nomenclaturas, bem como podem incorporar padrões internacionais ou uma estrutura de modelo de maturidade em seu conteúdo. Assim, optou-se doravante por designá-los genericamente como *modelos*, para generalizar os sistemas, modelos, guias, boas práticas e *frameworks*.

O universo da segurança cibernética está em constante evolução, exigindo a incorporação de novas dimensões no contexto organizacional a ser avaliado. Isto impõe a elaboração de critérios e indicadores para avaliar o estágio de maturidade da instituição. Entretanto, as diferenças conceituais acerca do objeto de segurança levam a uma maior ou menor abrangência desses instrumentos de avaliação. Por exemplo, o foco da segurança da informação são os mecanismos e a informação em si, enquanto a segurança cibernética é mais ampla, estendendo-se aos aspectos técnicos, infra estruturais, humanos e estratégicos necessários para assegurar o alcance dos objetivos (LE; HOANG, 2017).

As buscas na literatura científica foram conduzidas no *Google Scholar, ResearchGate, IEEE, Emerald, ScienceDirect e Academia.edu*, que reúnem artigos de revistas, conferências, relatórios, entre outros. As premissas consideradas nessa busca levaram em consideração os modelos disponíveis em fontes abertas (TEICHERT, 2019); as pesquisas publicadas em idioma inglês ou na língua nativa (REA-GUAMAN *et al.*, 2017); o alinhamento com as definições previamente levantadas nos documentos, normas e padrões internacionais (AZMI; TIBBEN; WIN, 2018); o acesso ao documento original na íntegra e dentro do cronograma estabelecido para a pesquisa (RAHIM *et al.*, 2015).

Os principais modelos levantados na literatura e pertinentes ao escopo desta pesquisa estão descritos no Quadro 2.

Quadro 2 – Principais modelos

Nr	Modelo	Autoria	Objetivos	Público-alvo	Descrição do modelo
1	CMM	SEI-Carnegie-Mellon	Desempenho de software	Organizações privadas	O *Capability Maturity Model* (CMM) foi publicado em 1992, pelo *Software Engineering Institute* da Universidade Carnegie Mellon, com o propósito de prover um método para avaliar a capacidade das empresas desenvolvedoras de software (PAULK *et al.*, 1993). O modelo define níveis e áreas de processos correspondentes, em cinco níveis de maturidade. É considerado descritivo, pois descreve os atributos principais esperados em uma organização para caracterizar um determinado nível de maturidade (PAULK *et al.*, 1993). O CMM permite avaliar a qualidade do software e apoiar seus desenvolvedores a melhorar os processos de forma contínua (LE; HOANG, 2017). Esse modelo pioneiro serviu de inspiração para que surgissem diversos outros, com ênfase às tecnologias, hardwares, softwares, dados, informações, redes, gerenciamento de risco, entre outras abordagens (BECKER *et al.*, 2010; PÖPPELBUSS; RÖGLINGER, 2011).
2	CMMI	SEI/CMMI-ISACA	Qualificar a capacidade das empresas de	Organizações contratadas	O *Capability Maturity Model Integration* (CMMI) foi o sucessor do modelo CMM, sendo desenvolvido para o Departamento de Defesa dos EUA, pelo *Software*

Nr	Modelo	Autoria	Objetivos	Público-alvo	Descrição do modelo
			software contratadas pelo governo dos EUA		*Engineering Institute* da Universidade de Carnegie Mellon (USA), com o propósito de avaliar a qualidade e a capacidade das empresas de software contratadas pelo governo norte-americano, especialmente no setor de softwares. O modelo derivou outros, como o *Software Capability Maturity Model* (SW-CMM) e o *Systems Engineering Capability Maturity Model* (SE-CMM), utilizado pela Agência Nacional de Segurança (NSA) dos EUA, lançado em 2001. Diferentemente dos outros modelos, o CMMI é uma abordagem para o desenvolvimento de produtos e serviços (CMMI-DEV V1.3), a gestão de serviços (CMMI-SVC V1.3) e a aquisição de produtos e serviços (CMMI Acquisition V1.3). Entretanto, o modelo não se estende sobre as matérias de segurança, a exemplo do *Systems Security Engineering* (SSE-CMM). Em 2018, foi lançado um programa de evolução e adaptação às melhores práticas para as novas ameaças, denominado *The CMMI Cybermaturity Plataform* A nova plataforma inclui opções de alinhamento ao COBIT 5, ao ISO/IEC 27000, ao CSF-NIST, ao C2M2 e ao ISC (BROWN, 2018; ENGLBRECHT; MEIER; PERNUL, 2020).
3	ISO/IEC 27000	ISO/IEC	Gerenciamento da Segurança da Informação por padrões de segurança	Organizações em geral	A ISO/IEC 27000 (*International Organization for Standardization/International Electrotechnical Comission*), inicialmente publicada em 2005, consiste em uma família de padrões acerca da segurança da informação. Essas normas derivam de um código de boas práticas do governo britânico para a gestão da Segurança da Informação. No Brasil, a norma foi reconhecida pela Associação Brasileira de Normas Técnicas – ABNT, recebendo o código ABNT NBR ISO/IEC 27000:2018, em sua última versão. A norma ISO/IEC 27000:2018 fornece a visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27000, sendo aplicável em ampla gama de organizações (ISO/IEC, 2018).
4	COBIT5	ISACA	Administrar a governança de TI como alicerce da segurança cibernética	Organizações em geral	Na mesma linha da ISO/IEC 27000, o COBIT (*Controls Objective for Information and related Technology*) também estabelece padrões para o controle de processos em áreas distintas, bem como um modelo de maturidade para a identificação do estágio atual da organização. O COBIT foi criado pela ISACA, um grupo de auditores norte-americanos, especializados em avaliação de sistemas de tecnologia da informação (ISACA, 2020).
5	ISA/IEC 62443 (ISA-99)	ISA	Estabelece controles para o setor de automação	Organizações em geral	Nos EUA, a ISA/IEC 62443, também denominada ISA-99, da *International Society of Automation*, oferece uma série de padrões de controle de sistemas industriais, com ênfase aos processos de

Nr	Modelo	Autoria	Objetivos	Público-alvo	Descrição do modelo
			industrial e sistemas de controle		automação. O modelo dispõe de um padrão especialmente voltado para os requisitos técnicos para a segurança cibernética (INTERNATIONAL SOCIETY OF AUTOMATION, 2018).
6	CIS CSC	SANS *Institute*	Estabelecer controles para assegurar a segurança de sistemas e dados contra ataques cibernéticos	Organizações em geral	Outro padrão de referência é o CIS-CSC, do *Center for Internet Security Critical Security Controls.* Suas publicações contêm guias de melhores práticas para a segurança computacional, denominadas de *Consensus Audit Guidelines,* com base na colaboração de agências governamentais dos EUA. Assim como o modelo descrito na ISA/IEC 62443, o CIS CSC estabelece controles críticos necessários para a redução de riscos e de ataques (CIS, 2020).
7	ISM2	PRISMA-NIST	Revisar os requisitos complexos de segurança da informação e a postura de um programa federal de segurança da informação	Organizações governamentais	O modelo ISM2 (*Information Security Maturity Model*) é resultante do Programa PRISMA (*Program Review for Information Security Management Assistance*). Em 2007, o *National Institute for Standards and Technology* (NIST) recebeu a tarefa de prover assistência técnica às agências governamentais, no que se refere à conformidade com os padrões e guias desenvolvidos para a proteção dos sistemas de informação, políticas, procedimentos e práticas. O modelo serve à avaliação dos níveis de segurança cibernética de uma organização e apoia a série de documentos produzidos no âmbito do NIST. Sua criação tem como base o CMM, pelo *Software Engineering Institute* (SEI) (BOWEN; KISSEL, 2007). A metodologia é qualitativa, aplicada através da condução de entrevistas, reuniões e as informações fornecidas pelo pessoal de interesse necessário para realizar a avaliação.
8	ISM3	The ISM3 Consortium	Prevenir ou mitigar ataques, erros, e acidentes que possam comprometer a segurança dos sistemas de segurança da informação e os processos organizacionais	Organizações privadas	O modelo ISM3 (*Information Security Management Maturity Model*) é um padrão orientado por processo que usa os níveis de maturidade da Gestão da Segurança da Informação para prevenir ou mitigar ataques, erros e acidentes que possam comprometer a segurança dos sistemas de segurança da informação e os processos organizacionais apoiados pelo seu uso. O modelo foi desenvolvido pelo *ISM3 Consortium* em 2007, em parceria com instituições de diferentes países. Suas práticas e conjuntos de processos estão divididos por natureza: Geral, Gestão Estratégica, Gestão Tática e Gestão Operacional. O modelo foca na gestão de métricas para a segurança da informação, mas não lida de maneira direta com a questão da segurança cibernética (BROWN, 2018).
9	C2M2	SEI-Carnegie-Mellon	Avaliar a implementação e gerenciamento nas Infraestruturas	Organizações em geral	O C2M2 (*Cybersecurity Capability Maturity Model*) foi desenvolvido pelo *U.S. Department of Energy* (DOE), para o uso em empresas do setor energético, em 2014. Deste modelo, duas versões para o setor de energia foram derivadas:

Nr	Modelo	Autoria	Objetivos	Público-alvo	Descrição do modelo
			Críticas		*Electricity Subsector C2M2* (ES-C2M2) e o *Oil and Natural Gas Subsector* C2M2 (ONG-C2M2) (CHRISTOPHER et al., 2014). Para o setor de serviços de tecnologia da informação, o C2M2 for *Information Technology Services* (C2M2 IT) foi publicado em 2015 e, como os anteriores, deriva do C2M2 original. O modelo está organizado em dez domínios, que reúnem práticas de segurança cibernética, sendo estes agrupados por objetivos. Para cada objetivo, as práticas estão ordenadas por um indicador de nível de maturidade (CURTIS; MEHRAVARI; STEVENS, 2015).
10	CSF	NIST	Melhoria da gestão de riscos cibernéticos nas infraestruturas críticas	Organizações em geral	O modelo CSF-NIST (*Cybersecurity Framework - National Institute of Standards and Technology*) foi publicado em 2014 e atualizado em 2018, organizando atividades de segurança da informação em cinco categorias, denominadas de camadas (*tiers*), com a possibilidade de progressão entre os níveis. Tem por propósito gerir riscos cibernéticos, ressaltando a necessidade de planejamento para a recuperação em caso de ataques, considerando os riscos cibernéticos como parte de processos de gestão de risco da organização. Assim como o ISM2, o CSF-NIST deriva outros documentos publicados pelo NIST. O modelo é o resultado de uma lista de funções, categorias, subcategorias e suas respectivas referências informativas que descrevem atividades de segurança cibernética específicas que são comuns aos setores de infraestrutura crítica. (NIST, 2018).
11	IAMM	CESG	Assistir a estratégia de TIC do governo do Reino Unido	Organizações governamentais	O modelo IAMM (*Information Assurance Maturity Model*) foi criado em 2008 e atualizado pelo *National Technical Authority for Information Assurance* e utilizado pelo *National Cyber Security Centre* (UK). Nesse modelo, as organizações podem efetuar sua autoavaliação através do *IA Assessment Framework* (IAAF). Assim, o IAMM e o IAAF provêm o modelo para assistir a estratégia de tecnologia da informação do governo do Reino Unido, contendo objetivos e processos. O modelo considera a informação como um ativo-chave do governo e incumbe agentes *Senior Information Risk Onwers* e *Information Asset Onwers* de serem responsáveis pela proteção adequada dos dados coletados, processados e armazenados em seus departamentos (CESG, 2015).
12	CAF	NCSC	Avaliar medidas técnicas e organizacionais para gerir os riscos de segurança de redes e dos sistemas de	Organizações governamentais	O *Cyber Assessment Framework* (CAF), desenvolvido pelo *National Cyber Security Centre* (NCSC), é um método de avaliação do Reino Unido para que as medidas técnicas e organizacionais sejam apropriadas e proporcionais para gerir os riscos de segurança de redes e dos sistemas de informação para operadores de serviços essenciais. O NCSC é a

Nr	Modelo	Autoria	Objetivos	Público-alvo	Descrição do modelo
			informação		autoridade técnica nacional que promove a colaboração entre o governo, indústria e academia, com o propósito de oferecer a defesa primária para as redes do governo contra ataques cibernéticos (NCSC, 2018). As autoridades competentes verificam em que medida os operadores de serviços essenciais estão alcançando os resultados especificados pelos princípios do modelo.
13	NCSG	ITU	Nortear princípios para o desenvolvimento de uma estratégia nacional de segurança cibernética	Organizações governamentais	O *National Cybersecurity Strategy Guide* (NCSG) é uma publicação em cooperação do *International Telecommunication Union* (ITU), com o Banco Mundial, o *Commonwealth Secretariat* (ComSec) e o *Cooperative Cyber Defence Centre of Excellence* da OTAN (NATO CCDCOE), entre outras instituições (ITU, 2018). Seu conteúdo tem o propósito de prover um modelo útil, flexível e de fácil compreensão para líderes e tomadores de decisão no desenvolvimento de uma estratégia nacional de segurança cibernética. O Guia se propõe a organizar e priorizar aspectos de governança, de políticas, de temas organizacionais, técnicos e legais, com base em modelos e outras referências do setor. Sua estrutura condiz com os modelos de maturidade previamente apresentados, mas não oferece um modelo de avaliação do nível da estratégia

Fonte: autoria própria

3.1 Escolha do modelo referência

Esta pesquisa adotou o modelo CSF-NIST como referência. O modelo explora uma seleção de controles da NIST, decorrente da SP 800-53, para a gestão de riscos cibernéticos em infraestruturas críticas. Em sua segunda versão em 2018, o modelo se baseou em cinco padrões internacionais: CIS CSC; COBIT 5; ISA 62443-2: 2009; ISO/IEC 27000:2013; e NIST SP 800-53 ver. 4, sendo a ISO/IEC 27000. Deste modo, suas atividades se alinham às necessidades reconhecidas no ambiente corporativo, incluindo os riscos de segurança cibernética como parte dos processos para a gestão de riscos de uma organização.

O CSF-NIST é aplicável aos setores público ou privado, devido ao seu caráter customizável, focado na melhoria da segurança e resiliência para cada organização. Além disso, o modelo apresenta aderência aos marcos regulatórios nacionais, pois atende às necessidades mencionadas no Art. 12 da PNSI, de competência do GSI, referentes ao Inciso VII. De igual forma, é possível relacionar aspectos do modelo ao Art. 17, de competência dos órgãos e entidades da APF, nos Incisos II, VII e VIII.

A estrutura do CSF-NIST consiste em três partes. A primeira diz respeito a uma estrutura básica, composta por conceitos comuns entre

setores e infraestruturas críticas, em que estão um conjunto de atividades, resultados e referências informativas de segurança cibernética. Na segunda parte, quatro níveis de implementação da estrutura descrevem o grau em que a instituição se encontra, em relação ao gerenciamento de riscos cibernéticos: parcial, risco informado, reproduzível e adaptável. A terceira parte se destina à avaliação da instituição, estabelecendo um alinhamento entre funções, categorias e subcategorias, com base nos objetivos institucionais, sua tolerância aos riscos e os recursos disponíveis na organização. Esta parte também serve à identificação do seu *status* atual ou desejado, seja local ou global.

O CSF-NIST se estrutura em cinco funções, agrupadas por objetivos. Essas funções se subdividem em 23 categorias e 108 subcategorias. A nomenclatura de sua estrutura foi adaptada, de "*objetivos*" a "*critérios*", de "*categorias*" a "*subcritérios de 1º nível*" e de "*subcategorias*" a "*subcritérios de 2º nível*", para facilitar a transição do modelo à estrutura hierárquica do AHP.

É importante ressaltar que o CSF-NIST não sugere um grau de importância ou um roteiro de implementação. Sua organização é funcional e diz respeito a um conjunto de atividades. À medida em que for necessário compor as atividades para a avaliação, outras categorias, subcategorias e referências informativas podem ser adicionadas pela instituição, se necessário. O CSF-NIST também apresenta referências informativas para cada subcategoria, com base em diferentes normas internacionais, permitindo esclarecimentos adicionais ou as adaptações necessárias a cada instituição.

Em síntese, o CSF-NIST foi considerado o modelo adequado para a adaptação dos critérios e subcritérios para monitoramento e avaliação da segurança cibernética em uma instituição pública ou privada, uma vez que se destaca por aspectos relevantes a considerar:

- Ampliação da compreensão tradicional de segurança da informação, com foco na confidencialidade, integridade e disponibilidade da informação. A segurança de seu escopo diz respeito aos aspectos técnicos, bem como aos recursos humanos evolvidos, às políticas e programas, ao *core business* da organização, a sua estrutura e comunicação com agentes internos e externos;
- Desenvolvimento para o uso comunitário com o propósito de auxiliar na gerência dos riscos cibernéticos de infraestruturas críticas, em vista da essencial importância para os governos e para a sociedade que dela depende;
- Requisitos oferecidos para um contexto plural, pautado em boas práticas, normas internacionais e diretrizes, oferecendo subsídios sobre quais matérias e requisitos devem constar nas preocupações de uma organização no enfrentamento do ambiente cibernético;

- Estrutura fragmentada para a produção de resultados para cada delimitação, para as funções, categorias e subcategorias;
- Constante atualização através de guias, melhores práticas e conhecimentos que compõem o fundamento de seu conteúdo, oriundos do *feedback* da indústria e das novas necessidades tecnológicas envolvendo ameaças, riscos e soluções;
- Ampla aceitação acadêmica por conta da inclusão de trabalhos de pesquisa e discussão entre especialistas, mantendo o seu conteúdo atual e, principalmente, relacionável entre outras ferramentas.

4 Processo de Análise Hierárquica (AHP)

Nesta Seção é explorado o método AHP e suas aplicações em políticas públicas, conforme registra a literatura científica, através de artigos e pesquisas em geral. O AHP se destina ao apoio à decisão multicritério, sendo utilizado no auxílio a problemas complexos. Com base em preferências colhidas junto à especialistas, essas avaliações são transformadas em pesos para a tomada de decisão.

4.1 O AHP aplicado em políticas públicas

Uma parcela desta pesquisa versa sobre o aperfeiçoamento de uma política pública, através do uso de um método de Pesquisa Operacional. Esse aperfeiçoamento foi publicamente requerido, quando o Decreto Nº 9.637 solicitou a ampla participação da sociedade e dos órgãos e das entidades do Poder Público para contribuírem com a construção da Estratégia Nacional de Segurança da Informação. No mesmo documento, foi também formalmente descrita ao Gabinete de Segurança Institucional da Presidência da República (GSI-PR) a tarefa de estabelecer critérios que permitam o monitoramento e a avaliação da execução da PNSI e de seus instrumentos. Esta necessidade específica de criar uma estrutura de critérios para o monitoramento e avaliação de uma política pública é assunto específico da Pesquisa Operacional e, em particular, aos métodos de apoio à decisão multicritério.

As políticas públicas são instrumentos fundamentais do Estado para promover o bem-estar da sociedade, pois asseguram a prestação de serviços aos seus cidadãos. A avaliação de uma política pública é a etapa final do ciclo que se inicia com a sua criação, permitindo o controle de todo o processo que aprimora as suas atividades (BRASIL, 2013). Em 2018, o Governo Federal lançou uma cartilha para orientar gestores e técnicos na formulação e avaliação de políticas públicas (BRASIL, 2018). O conteúdo da cartilha apresentou seis passos essenciais dessa gestão: (1) diagnóstico do problema; (2) objetivos, ações e resultados; (3) desenho e estratégia de implementação; (4) impacto orçamentário e financeiro; (5) estratégia de construção de confiança e suporte; e (6) monitoramento,

avaliação e controle. Conforme descrito no capítulo introdutório, esta pesquisa objetiva a avaliação da implementação da PNSI.

A governança de um programa de segurança cibernética envolve elementos complexos, que incluem a tomada de decisão em diferentes níveis. No caso brasileiro, em função do escopo governamental do PNSI, esses elementos ultrapassam os limites de uma organização, envolvendo um espectro mais amplo de pessoas e instituições. As políticas formuladas passam por um processo mais burocrático, conferindo maior complexidade à governança e, por consequência, as decisões que dela decorrem.

Nesse contexto, é preciso adotar procedimentos que levem ao auxílio do processo de tomada de decisão. Para Saaty (2002), esse processo requer conhecer o problema, as suas necessidades e propósito, bem como os seus critérios, subcritérios e possíveis alternativas que o solucione. Em decorrência disto, Saaty (1980) propôs o método AHP, que se caracteriza pela abordagem multicritério de tomada de decisão. O método fragmenta decisões complexas sob uma estrutura hierárquica, desde o objetivo principal no topo, até as alternativas, interligados por níveis de critérios e subcritérios, todos avaliados de forma pareada em relação aos seus níveis imediatamente superiores.

O AHP tem sido utilizado com sucesso para a avaliação de políticas públicas, incluindo as relacionadas à segurança da informação. Hassan e Lee (2019) aplicaram o AHP para avaliar política de governança digital no setor público do Paquistão. Esse conceito de governança digital ou eletrônica (i.e. *e-Governance*) se refere à utilização da internet para veicular informações governamentais e prover serviços públicos aos cidadãos. Os autores selecionaram fatores críticos de sucesso (FCS) para criar uma estrutura hierárquica do problema. Diversas entrevistas com as partes interessadas foram implementadas, com base na escala de Saaty, para conhecer sua perspectiva sobre a estrutura proposta e determinar a importância relativa sobre os FCS.

Em uma organização, o estabelecimento de estratégias e políticas em segurança da informação começam, geralmente, com um diagnóstico do nível de maturidade em que se encontra. Nasser et al. (2018) utilizaram o AHP para avaliar a gestão de segurança da informação, a partir dos controles da norma ISO 27000:2018.

Katsianis et al. (2018) utilizaram o AHP *fuzzy* para priorizar questões tecnológicas e socioeconômicas que podem influenciar a implantação e a adoção do projeto SHIELD no âmbito governamental da União Europeia. Esse projeto visa a concepção e desenvolvimento de uma nova estrutura de segurança cibernética, com o objetivo de oferecer segurança como serviço em um ambiente de telecomunicações.

Bernieri et al. (2016) exploraram o AHP para auxiliar a tomada de decisão de operadores de segurança de redes, em relação à melhor

alternativa de recuperar o estado seguro de uma infraestrutura crítica sob ataque. Os autores simularam um ataque cibernético desferido contra sensores de níveis de água de um sistema de distribuição. Devido à sua relevância, esse tipo de sistema, juntamente com redes elétricas e gasodutos podem ser analisados sob a ótica do AHP. Sistemas de controle, algoritmos de detecção de falhas e sistemas de detecção de intrusão são considerados essenciais para a proteção de infraestrutura crítica.

Syamsuddin (2013) usou o AHP para orientar tomadores de decisão que avaliam o desempenho da política de segurança da informação. O autor destacou que o aumento do número e no impacto de ataques cibernéticos em ativos de informação resultou na crescente conscientização entre os gerentes de que o ataque à informação é, na verdade, um ataque à própria organização. O autor propôs um modelo específico de avaliação da segurança da informação para níveis de gerenciamento. A estrutura do AHP foi desenvolvida em uma estrutura hierárquica contendo quatro critérios que representam os quatro principais aspectos da segurança da informação: gestão, tecnologia, economia e cultura organizacional. No último nível hierárquico, três alternativas foram consideradas: a confidencialidade das informações, a integridade dos sistemas, disponibilidade dos serviços, que representam uma solução estratégica para implementação dos sistemas de segurança da informação. Os resultados mostraram a preferência pela disponibilidade dos serviços, seguida de confidencialidade e da integridade. As descobertas contribuem para o desenvolvimento de estratégias para melhorar a eficácia da política de segurança da informação na organização.

Badie e Lashkari (2012) aplicaram o AHP para avaliar os riscos inerentes à segurança da informação, com foco no fator humano, de forma a orientar a elaboração de planos que ampliem a conscientização dos usuários sobre o tema. Os autores também destacam a importância em relação à confidencialidade das informações, integridade dos sistemas e disponibilidade dos serviços, nas atividades de segurança da informação. Os autores afirmam que qualquer sistema de segurança, não importa o quão bem projetado e implementado, ainda depende do fator humano para o seu adequado desempenho. Os resultados indicaram o treinamento do usuário com o principal efeito positivo para reduzir a falta de conscientização de segurança da informação.

O AHP também auxilia na tomada de decisão estratégica, tanto no âmbito governamental quanto corporativo. Bhushan e Rai (2007) utilizaram o AHP para auxílio da decisão na área de negócios, defesa e governança. Os autores aplicaram o método para a seleção de fornecedores à avaliação de sistemas de armas, para a gestão de projetos

de apoio à decisão em desastres naturais e para a seleção de fatores que afetam a segurança nacional.

Outros métodos de apoio à decisão em políticas de segurança da informação também têm sido identificados na literatura científica recente. Erdoğan et al. (2019) propôs uma metodologia de tomada de decisão com múltiplos critérios, modelados por conjuntos *fuzzy* hesitantes, que oferece aos especialistas uma flexibilidade adicional no uso de termos linguísticos para avaliar os critérios e alternativas para determinar a melhor tecnologia de segurança cibernética. Yuen (2019) explorou conceitos de sustentabilidade e confiabilidade de um sistema de segurança da informação através de um método multicritério denominado Processo de Rede Cognitiva Primitiva (PCNP), para a tomada de decisão sobre investimentos em segurança cibernética.

O método AHP foi adotado como a referência às avaliações de políticas públicas nesta pesquisa. A escolha por um modelo de apoio à decisão consagrado na literatura decorre de alguns fatores. Inicialmente, verificou-se o uso prévio e recente na avaliação de políticas públicas em diferentes países e em renomados periódicos. Também é possível destacar uma série de vantagens do método: sua estrutura multicritério, permitindo avaliar um problema sob múltiplos pontos de vista; sua simplicidade de cálculo e programação, a partir de equações oriundas da álgebra linear; sua simplicidade lógica que facilita a aceitação por parte de tomadores de decisão, não necessariamente familiarizados com modelos matemáticos; seu processo de autoavaliação de consistência, que permite validar ou não os resultados dos especialistas. Entre as suas limitações, cabe destacar a dependência de especialistas para a realização das avaliações paritárias dos critérios, subcritérios e alternativas do problema. Também cabe mencionar que um problema com elevada quantidade de variáveis potencializa a quantidade de avaliações paritárias, o que pode comprometer a consistência lógica e o elevado tempo de avaliação dos especialistas.

4.2 Detalhamento do método AHP

O AHP é um método de apoio à decisão multicritério, útil para a solução de problemas complexos (WIND; SAATY, 1980). O AHP é basicamente utilizado para definir uma ordem de prioridade das alternativas capazes de solucionar o problema. O método adota a seguinte sequência de procedimentos: (1) definir o objetivo, os critérios de avaliação, eventuais subcritérios e possíveis alternativas, estabelecendo uma estrutura hierárquica ao problema; (2) comparar os elementos de decisão de forma paritária em cada nível da estrutura hierárquica, em relação ao nível superior, com base em uma escala específica; (3) calcular os pesos relativos dos elementos de decisão nos diversos níveis

hierárquicos e, por fim, (4) ordenar as alternativas de decisão a partir da agregação dos pesos dos elementos de decisão.

A estrutura hierárquica do problema pode ser ilustrada pela Figura 1, que descreve um problema genérico com quatro critérios e três alternativas. Essa estrutura define níveis hierárquicos entre o objetivo no topo e as alternativas na base, que permitem solucionar o problema. Os níveis intermediários podem ser formados por critérios e subcritérios, em quantos níveis forem necessários para descrever a estrutura do problema.

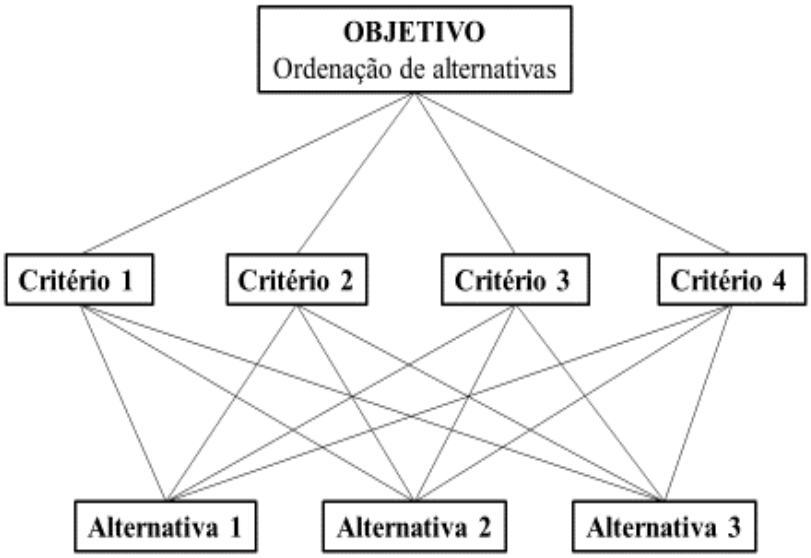

Figura 1 - Estrutura hierárquica genérica de um problema.

Fonte: Adaptado de Saaty (1980).

O AHP requer avaliações para os critérios, eventuais subcritérios e alternativas, efetuadas para um nível acima em sua estrutura. Essas avaliações são paritárias e compõem matrizes com valores da escala proposta por Saaty & Vargas (1980), conforme a Figura 2.

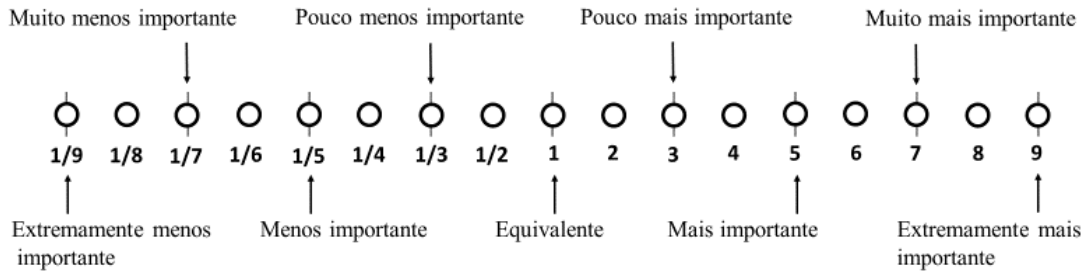

Figura 2 - Escala de avaliação paritária.

Fonte: adaptado de Saaty (1980)

No método de comparação paritária, os critérios, eventuais subcritérios e alternativas são avaliados por especialistas ou tomadores de decisão. Essas avaliações geram uma matriz quadrada para cada nível hierárquico, tendo por referência o nível hierárquico imediatamente superior, conforme a Equação (1).

$$A = \begin{bmatrix} 1 & a_{12} & \dots & a_{1n} \\ 1/a_{12} & 1 & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \dots & 1 \end{bmatrix} \quad (1)$$

Na matriz A, $a_{ij}=1/a_{ji}$ e quando i=j, $a_{ij}=1$, por se tratar de elementos equivalentes, tornando-a uma matriz recíproca de avaliações paritárias. Definidas as matrizes, os procedimentos subsequentes seguem conceitos oriundos da álgebra linear. Na sequência são efetuados os cálculos do AHP, com a finalidade de obter os pesos relativos dos critérios e subcritérios, além dos cálculos da consistência lógica das avaliações efetuadas. Na Equação (2) são calculados os pesos w_i de cada elemento da matriz. Essa variável w_i corresponde ao autovetor dos elementos de uma matriz, sendo obtido de maneira simplificada através da média aritmética entre a raiz *n* do produto das avaliações a_{ij} e a soma desses resultados, para cada linha. O procedimento de cálculo das Equações (2) a (6) foi proposto por Liu e Lin (2016).

$$w_i = \frac{\left(\prod_{j=1}^{n} a_{ij} \right)^{1/n}}{\sum_{i=1}^{n} \left(\prod_{j=1}^{n} a_{ij} \right)^{1/n}} \quad (2)$$

Em seguida, deve ser calculado o λ_{max}, que corresponde ao autovalor máximo da matriz recíproca, sendo obtido através das Equações (3) e (4).

$$A^s = \begin{bmatrix} 1 & a_{12} & \dots & a_{1n} \\ 1/a_{12} & 1 & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \dots & 1 \end{bmatrix} \times \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} w_1' \\ w_2' \\ \vdots \\ w_n' \end{bmatrix} \quad (3)$$

$$\lambda_{\max} = (1/n) \times (w_1^{'} / w_1 + w_2^{'} / w_2 \cdots + w_n^{'} / w_n) \quad (4)$$

Essa variável λ_{max} é necessária para os cálculos posteriores do AHP, que incluem o Índice de Consistência (IC), o Índice Randômico (IR), calculado com base na Tabela 1 de referência com a razão da matriz (quantidade de linhas/colunas da matriz recíproca) e a Razão de Consistência (RC), conforme as Equações (5) e (6).

$$IC = \frac{\lambda_{\max} - n}{n-1} \quad (5)$$

$$RC = \frac{IC}{IR} \quad (6)$$

Tabela 1 – Índices aleatórios

Razão da matriz	1	2	3	4	5	6	7	8	9	10
Índice Aleatório (IR)	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Fonte: adaptado de Bhaskar et al (2019).

A RC indica a validação interna do método AHP, sendo utilizada para verificar a consistência lógica das avaliações paritárias de cada matriz, sendo considerado o valor de 10% como aceitável. (SAATY, 1983). Para Forman (1993), a inconsistência das avaliações decorre dos erros de julgamento humano, de parcialidade nas avaliações e de uma compreensão perfeita dos especialistas acerca do problema avaliado. Aquele autor exemplifica essa inconsistência no ambiente esportivo, em que não raro um time "A" vence um time "B" e este time "B" vence um time "C", porém o time "A" perde para o time "C". Em relação às escolhas ou preferências em problemas de pesquisa essa inconsistência é indesejável e, para valores de RC superiores a 10%, é recomendável uma nova rodada de avaliações com o especialista, até que seja atendida essa condição de validade. Na prática, a repetição desse procedimento pode ser inexequível, diante da indisponibilidade de tempo e de recursos. Em função disto, diversos autores propuseram técnicas com simulação de Monte Carlo e procedimentos estatísticos, capazes de mitigar essas limitações provocadas por inconsistência das avaliações, para ajustar a coleta de dados ao mundo real (ACZÉL; SAATY, 1983; MOMANI; AHMED, 2011; SAATY, THOMAS L; VARGAS, 2012; VARGAS, 1982).

5 Aplicação

Esta seção apresenta a execução das Etapas 6 a 9 da pesquisa, que correspondem à elaboração dos questionários de avaliação, à coleta dos dados aos estudos de caso, ao cálculo dos pesos dos critérios e subcritérios e ao cálculo das Razões de Consistência para a validação do modelo.

Foram utilizados dois questionários. O primeiro se referiu à metodologia do AHP, para o cálculo dos pesos dos critérios e subcritérios (1º e 2º níveis), adaptados do CSF-NIST, e validação interna do processo com as Razões de Consistência. O segundo questionário foi utilizado para a coleta dos dados referentes à aplicação nas instituições escolhidas para o teste, qualificando o *status* de maturidade cada subcritério de 2º nível. Foram selecionadas duas instituições: um banco público brasileiro e uma empresa de auditoria. Por necessidade de concisão do artigo, o questionário foi omitido.

A estrutura do primeiro questionário segue basicamente a hierarquia do problema, segundo o AHP. Para cada nível, são efetuadas avaliações paritárias entre as variáveis, segundo a escala de Saaty. No início do questionário, foi utilizado um exemplo de avaliação para orientar o especialista no preenchimento de seus julgamentos, conforme a Figura 3. Pergunta-se ao respondente a importância de um determinado critério em relação a outro do mesmo nível hierárquico. As perguntas, neste modelo, são feitas da linha da matriz de avaliações em relação a sua coluna. Assim, o critério A (da linha), na esquerda da escala, será comparado com o critério B (da coluna), na direita da escala. Se o critério A for considerado "muito mais importante" que o critério B, então ele recebe o grau "5" da escala.

A avaliação paritária entre as variáveis resulta em uma da matriz de importância relativa entre elas, conforme ilustrado na Tabela 2. As células hachuradas em cor cinza não requerem avaliações, por corresponderem aos valores inversos, de tal forma que $a_{ji} = 1/a_{ij}$, em que "i" é a linha da matriz e "j" a coluna.

Tabela 2 – Avaliações do subcritério Gerenciamento de Ativos

Gerenciamento de Ativos	ID AM 1	ID AM 2	ID AM 3	ID AM 4	ID AM 5	ID AM 6
ID AM 1	1	3	3	5	1	1/3
ID AM 2		1	1	3	1	1/3
ID AM 3			1	3	1/3	1/5
ID AM 4				1	1/5	1/5
ID AM 5					1	1/3

Gerenciamento de Ativos	ID AM 1	ID AM 2	ID AM 3	ID AM 4	ID AM 5	ID AM 6
ID AM 6						1

Após a coleta dos dados, as Equações (2) a (6) de cálculo do AHP foram efetuadas para cada matriz, indicando os pesos de cada variável e as Razões de Consistência dos seus julgamentos.

Após o processamento do primeiro questionário, foi transmitido o segundo, para a coleta do nível de maturidade da instituição, de acordo com a percepção do respondente. Foram atribuídas notas de "1" a "5" aos 108 subcritérios de 2º nível, em que "1" indicava o menor nível de maturidade e "5" o maior. Caso o item de avaliação não fosse aplicável à instituição, o respondente deveria indicar "0". A soma ponderada de cada avaliação desse *status* de maturidade, com os pesos dos subcritérios de 2º nível, resultou no nível global de maturidade da instituição. Por necessidade de concisão do artigo, as matrizes de dados coletados foram omitidas.

5.1 Resultados

Este estudo de caso se refere a um banco público de relevância ao governo brasileiro. A organização dispõe de diversos produtos para a pessoa física e jurídica, bem como apoia o poder público na implantação de políticas públicas. A instituição, de abrangência nacional, possui mais de mais de 80 mil funcionários. Para uma instituição financeira, a segurança da informação e a manutenção da segurança cibernética são imperativas ao desempenho adequado e seguro de suas atividades.

O avaliador deste estudo de caso é graduado em ciência da computação e mestre em engenharia de sistemas e computação por instituições públicas de ensino superior. Possui especialização em segurança da informação em uma empresa privada e leciona sobre segurança de redes e sistemas operacionais em instituição de ensino.

A aplicação da Equação (2) do AHP, para cada matriz coletada junto ao avaliador, gerou pesos para cada variável. A Tabela 3 reúne esses pesos e os níveis de maturidade avaliados no primeiro estudo de caso.

Tabela 3 – Resultados do Estudo de Caso

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
ID - Identificar	0,19526401	AM – Gerenciamento de Ativos	0,25643021	ID.AM-1 Inventário de aparelhos e sistemas da organização;	0,206108	0,01032	5	0,051601
				ID.AM-2 Inventário de plataformas de software e aplicativos usados na organização;	0,109285	0,005472	5	0,02736

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				ID.AM-3 Mapeamento das comunicações organizacionais e fluxo de dados;	0,083573	0,004185	2	0,008369
				ID.AM-4 Catálogo de sistemas de informação externos;	0,040696	0,002038	2	0,004075
				ID.AM-5 Priorização de recursos com base em sua importância;	0,171623	0,008593	1	0,008593
				ID.AM-6 Estabelecimento de papéis e responsabilidades de segurança cibernética para a organização.	0,388715	0,019464	1	0,019464
		BE – Ambiente Corporativo	0,09427431	ID-BE-1 Papel da organização na cadeia de suprimentos;	0,111111	0,002045	4	0,008182
				ID-BE-2 Relevância da organização no seu ambiente de negócios;	0,111111	0,002045	2	0,004091
				ID-BE-3 Prioridades para a missão organizacional, objetivos e atividades;	0,333333	0,006136	2	0,012272
				ID-BE-4 Dependências e funções críticas para alcançar serviços críticos;	0,333333	0,006136	2	0,012272
				ID-BE-5 Requisitos de resiliência para apoiar a entrega de serviços críticos.	0,111111	0,002045	4	0,008182
		GV – Governança	0,25643021	ID-GV-1 Política de segurança cibernética organizacional;	0,099602	0,004987	5	0,024936
				ID-GV-2 Papéis e responsabilidades coordenadas com todos os parceiros;	0,099602	0,004987	3	0,014962
				ID-GV-3 Requisitos legais e regulatórios concernentes à segurança cibernética;	0,249484	0,012492	3	0,037476
				ID-GV-4 Processos de governança e gestão de riscos.	0,557865	0,027933	3	0,0838
		RA – Gerenciamento de Risco	0,25643021	ID-RA-1 Identificação e documentação de vulnerabilidade de bens;	0,059283	0,002968	3	0,008905
				ID-RA-2 Inteligência de ameaça cibernética;	0,161251	0,008074	1	0,008074
				ID-RA-3 Identificação e documentação de ameaças internas e externas;	0,39768	0,019912	1	0,019912
				ID-RA-4 Impactos potenciais do negócio e probabilidade;	0,161251	0,008074	1	0,008074
				ID-RA-5 Determinação de riscos a partir das ameaças, vulnerabilidades,	0,161251	0,008074	1	0,008074

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				probabilidades e impactos;				
				ID-RA-6 Priorizar respostas aos riscos.	0,059283	0,002968	1	0,002968
		RM – Estratégia de Gerenciamento de Risco	0,09427431	ID.RM-1 Processos para gestão de risco;	0,428571	0,007889	2	0,015779
				ID.RM-2 Determinação de uma tolerância de risco;	0,142857	0,00263	2	0,00526
				ID.RM-3 Determinação de risco da organização determinada pelo seu papel no seu ambiente e análise de risco de setor específico.	0,428571	0,007889	2	0,015779
		SC – Gerenciamento de Risco de Demanda	0,04216075	ID.SC-1 Processos de gestão de risco na cadeia de suprimentos cibernéticos;	0,371566	0,003059	2	0,006118
				ID.SC-2 Fornecedores e outros parceiros de sistemas de segurança da informação, componentes e serviços;	0,162244	0,001336	2	0,002671
				ID.SC-3 Contrato com fornecedores aderentes ao plano de gestão de riscos na cadeia de suprimentos cibernéticos;	0,347384	0,00286	2	0,00572
				ID.SC-4 Avaliações rotineiras com os fornecedores e outros parceiros;	0,07695	0,000633	2	0,001267
				ID.SC-5 Planejamento e testes de resposta e recuperação conduzidos com fornecedores e outros parceiros.	0,041857	0,000345	2	0,000689
PR - Proteger	0,46305701	AC – Gerenciamento de Identidade e Controle de Acesso	0,25643021	PR-AC-1 Identidades e credenciais emitidas, geridas, verificadas, revogadas e auditadas para aparelho autorizados, usuários e processos;	0,205811	0,024438	5	0,122192
				PR-AC-2 Acesso físico aos bens;	0,205811	0,024438	5	0,122192
				PR-AC-3 Gestão de acesso remoto;	0,074613	0,00886	5	0,044298
				PR-AC-4 Permissões de acesso e autorizações;	0,205811	0,024438	5	0,122192
				PR-AC-5 Integridade de rede;	0,205811	0,024438	1	0,024438
				PR-AC-6 Identidades comprovadas e ligadas a credenciais e avaliações em interações;	0,04763	0,005656	3	0,016967
				PR-AC-7 Usuários, aparelhos e outros bens autorizados de	0,054512	0,006473	3	0,019419

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				acordo com os riscos de transição				
		AT – Consciência e Treinamento	0,09427431	PR.AT-1 Usuários treinados e informados;	0,343888	0,015012	3	0,045037
				PR.AT-2 Tarefas e responsabilidades claras para usuários privilegiados;	0,128929	0,005628	2	0,011257
				PR.AT-3 Tarefas e responsabilidades claras dos demais interessados;	0,054367	0,002373	2	0,004747
				PR.AT-4 Tarefas e responsabilidades claras de executivos sêniores;	0,128929	0,005628	2	0,011257
				PR.AT-5 Tarefas e responsabilidades claras para a equipe física e de segurança cibernética.	0,343888	0,015012	2	0,030024
		DS – Segurança de Dados	0,25643021	PR.DS-1 Dados *at-rest*;	0,206271	0,024493	3	0,073479
				PR.DS-2 Dados *in-transit*;	0,206271	0,024493	3	0,073479
				PR.DS-3 Bens formalmente geridos;	0,089531	0,010631	4	0,042524
				PR.DS-4 Manutenção de capacidade adequada par garantir a disponibilidade;	0,206271	0,024493	2	0,048986
				PR.DS-5 Implementação de proteções contra vazamento de dados;	0,193511	0,022978	1	0,022978
				PR.DS-6 Mecanismos de checagem de integridade para avaliação de integridade de software, firmware e informação;	0,049435	0,00587	1	0,00587
				PR.DS-7Ambiente de teste e desenvolvimento separado do ambiente produtivo;	0,024355	0,002892	5	0,01446
				PR.DS-8 Mecanismo para a checagem de integridade para verificar integridade de *software*.	0,024355	0,002892	3	0,008676
		IP – Processos e Procedimentos de Proteção de Informação	0,09427431	PR.IP-1 Configuração de sistemas de controles da tecnologia da informação e industriais;	0,119921	0,005235	3	0,015705
				PR.IP-2 Sistema de desenvolvimento de ciclo de vida;	0,050059	0,002185	3	0,006556
				PR.IP-3 Processos de mudança na configuração de controles;	0,050059	0,002185	5	0,010927
				PR.IP-4 Backups de informações;	0,334281	0,014593	5	0,072964
				PR.IP-5 Políticas e regulações a respeito de ambientes físicos;	0,119921	0,005235	3	0,015705
				PR.IP-6 Destruição de	0,050059	0,002185	4	0,008741

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				dados conforme a política;				
				PR.IP-7 Melhoria de proteção de processos;	0,021783	0,000951	4	0,003804
				PR.IP-8 Compartilhamento da eficácia de tecnologias protetivas;	0,012095	0,000528	1	0,000528
				PR.IP-9 Gestão de planos de resposta e recuperação;	0,119921	0,005235	3	0,015705
				PR.IP-10 Testes de planos de resposta e recuperação;	0,021783	0,000951	3	0,002853
				PR.IP-11 Práticas e treinamentos do pessoal com segurança cibernética;	0,050059	0,002185	1	0,002185
				PR.IP-12 Plano de gestão de vulnerabilidade.	0,050059	0,002185	3	0,006556
		MA – Manutenção	0,04216075	PR.MA-1 Controle de manutenção e de reparos de bens organizacionais;	0,75	0,014642	4	0,058568
				PR.MA-2 Controle de manutenção remota de bens organizacionais.	0,25	0,004881	4	0,019523
		PT – Tecnologia Protetiva	0,25643021	PR.PT-1 Auditoria dos registros conforme a política organizacional;	0,281473	0,033423	3	0,100268
				PR.PT-2 Proteção e restrição de uso de mídia conforme a política organizacional;	0,050051	0,005943	5	0,029716
				PR.PT-3 Configuração de sistemas estritamente às capacidades essenciais;	0,105529	0,012531	5	0,062653
				PR.PT-4 Proteção de comunicações e controle de redes;	0,281473	0,033423	1	0,033423
				PR.PT-5 Mecanismos para alcance de resiliência.	0,281473	0,033423	2	0,066845
DE - Detectar	0,19526401	AE – Anomalias e Eventos	0,1047294	DE-AE-1 Patamar de operações de rede e fluxo de dados esperados para usuário e sistemas;	0,501067	0,010247	3	0,03074
				DE-AE-2 Análise de eventos detectados;	0,246083	0,005032	2	0,010065
				DE-AE-3 Dados dos eventos coletados e analisados;	0,10377	0,002122	2	0,004244
				DE-AE-4 Determinação de impacto dos eventos;	0,10377	0,002122	2	0,004244
				DE-AE-5 Estabelecimento de limites para alerta de incidentes.	0,045311	0,000927	2	0,001853
		CM – Contínuo Monitoramento de Segurança	0,6369856	DE.CM-1 Monitoramento de rede;	0,233503	0,029043	3	0,08713
				DE.CM-2 Monitoramento do ambiente físico;	0,233503	0,029043	2	0,058086
				DE.CM-3	0,040319	0,005015	1	0,005015

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				Monitoramento da atividade do pessoal;				
				DE.CM-4 Detecção de código malicioso;	0,233503	0,029043	3	0,08713
				DE.CM-5 Detecção de código móvel não autorizado;	0,097028	0,012068	3	0,036205
				DE.CM-6 Monitoramento de atividade de provedores de serviços externos;	0,053062	0,0066	3	0,0198
				DE.CM-7 Monitoramento de conexões não autorizadas;	0,053062	0,0066	3	0,0198
				DE.CM-8 Escaneamento de vulnerabilidades.	0,056019	0,006968	3	0,020903
		DP – Processos de Detecção	0,258285	DE.DP-1 Tarefas e responsabilidades definidas para detecção;	0,158835	0,008011	3	0,024032
				DE.DP-2 Atividades de detecção conforme os requisitos;	0,36376	0,018346	3	0,055037
				DE.DP-3 Testes de processos de detecção;	0,038311	0,001932	2	0,003864
				DE.DP-4 Comunicação de informação de detecção de eventos;	0,36376	0,018346	2	0,036692
				DE.DP-5 Melhoria de processo de detecção.	0,075334	0,003799	2	0,007599
RS - Responder	0,07320748	RP – Planejamento de Resposta	0,36376037	RS.RP-1 Execução de um plano de resposta durante ou após um incidente.	1	0,02663	2	0,05326
		CO – Comunicações	0,07533359	RS.CO-1 Tarefas e ordem de operações claras para a equipe em caso de necessidade de resposta;	0,231443	0,001276	2	0,002553
				RS.CO-2 Incidentes relatados consistentes com os critérios estabelecidos;	0,548853	0,003027	1	0,003027
				RS.CO-3 Informações compartilhadas consistentes com os planos de resposta;	0,125893	0,000694	1	0,000694
				RS.CO-4 Coordenação com stakeholders consistentes com os planos de resposta;	0,061828	0,000341	1	0,000341
				RS.CO-5 Compartilhamento voluntário.	0,031983	0,000176	1	0,000176
		AN – Análise	0,15883475	RS.AN-1 Investigação de notificações pelos sistemas de detecção;	0,111328	0,001295	3	0,003884
				RS.AN-2 Impacto dos incidentes;	0,049446	0,000575	1	0,000575
				RS.AN-3 Perícia;	0,416736	0,004846	3	0,014537
				RS.AN-4 Categorização dos incidentes;	0,046228	0,000538	1	0,000538
				RS.AN-5 Estabelecimento de processos para	0,376262	0,004375	1	0,004375

Critérios	Pesos Critérios	Subcritérios do 1º Nível	Pesos SC 1	Subcritérios do 2º Nível	Pesos SC 2	Pesos Finais	Maturidade	Resultado
				receber, analisar e responder às vulnerabilidades internas e externas.				
		MI – Mitigação	0,36376037	RS.MI-1 Contenção de incidentes;	0,178178	0,004745	3	0,014235
				RS.MI-2 Mitigação de incidentes;	0,751405	0,02001	3	0,06003
				RS.MI-3 Mitigação ou documentação de novas vulnerabilidades identificadas como riscos aceitos.	0,070418	0,001875	1	0,001875
		IM – Melhorias	0,03831093	RS.IM-1 Lições aprendidas incorporadas aos planos de resposta;	0,75	0,002103	2	0,004207
				RS.IM-2 Atualização das estratégias de resposta.	0,25	0,000701	1	0,000701

5.2 Análise

O gráfico da Figura 4 traduz em imagem as maturidades globais da última coluna "Resultado", na Tabela 3. Assim, é possível verificar que a variável "*PR-AC-1 Identidades e credenciais emitidas, geridas, verificadas, revogadas e auditadas para aparelhos autorizados, usuários e processos;*" foi a de maior maturidade na instituição avaliada. Os níveis de maturidade global decrescem do canto superior esquerdo ao inferior direito do gráfico, sendo as dimensões dos 108 retângulos proporcionais ao resultado final. O posicionamento do cursor sobre a sigla de cada variável, no gráfico, permite verificar o nível de maturidade global da variável. Esse gráfico, dessa forma, facilita a visualização por parte da instituição, acerca dos melhores e piores indicadores de maturidade. Esses resultados, em cada instituição, precisam ser reavaliados, preferencialmente através de uma comissão de autoavaliação que efetuou essa coleta de dados, para que medidas de aperfeiçoamento desses indicadores possam ser implementadas, com vistas ao melhoramento da segurança da informação e cibernética.

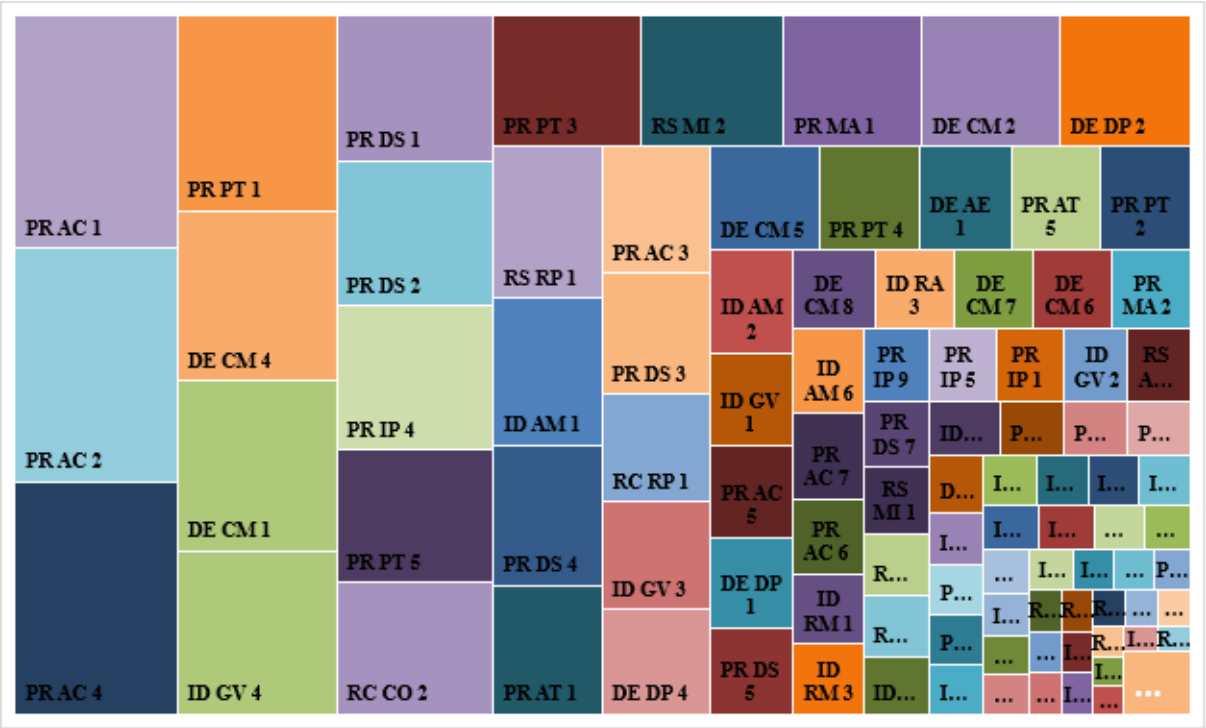

Figura 4 - Gráfico dos índices globais de maturidade do Estudo de Caso

As Equações (3) a (6) do AHP permitiram calcular as Razões de Consistência dos julgamentos do avaliador, conforme a Tabela 4. Os resultados indicados em cor vermelha trazem as RC iniciais com inconsistência, que requereram nova rodada de avaliação até atingir o novo RC, indicado logo abaixo. Os pesos considerados anteriormente, na Tabela 3, se referem às RC inferiores a 10%. De maneira geral, pode-se considerar que a consistência do avaliador foi muito boa, em decorrência da quantidade de avalições inconsistentes diante do total de julgamentos.

Tabela 4 – Razões de Consistência do Estudo de Caso

Critérios	RC dos Critérios	SC 1º Nível	RC dos SC 1º Nível	SC 2º Nível	RC dos SC 2º Nível
Identificar	RC= 0,0124	ID-AM	RC = 0,009375409	ID.AM-1 a ID.AM-6	RC= 0,04496589
		ID-BE		ID.BE-1 a ID.BE-5	RC = 0
		ID-GV		ID.GV-1 a ID.GV-4	RC=0,2251382 RC=0,01610639
		ID-RA		ID-RA-1 a ID-RA-6	RC=0,009375409
		ID-RM		ID-RM-1 a ID-RM-3	RC= 0
		ID-SC		ID-SC-1 a ID-SC-5	RC=0,04305356
Proteger		PR.AC	RC= 0,009375409	PR.AC-1 a PR.AC-7	RC = 0,0493148
		PR.AT		PR.AT-1 a PR.AT-5	RC=0,01242043
		PR.DS		PR.DS-1 a PR.DS-8	RC=0,01929838
		PR.IP		PR.IP-1 a PR.IP-12	RC=0,2497359 RC=0,02594748
		PR.MA		PR.MA-1 a PR.MA-2	RC = 0
		PR.PT		PR.PT-1 a PR.PT-5	RC=0,009365954

Critérios	RC dos Critérios	SC 1º Nível	RC dos SC 1º Nível	SC 2º Nível	RC dos SC 2º Nível
Detectar		DE.AE	RC= 0,03319922	DE.AE-1 a DE.AE-5	RC=0,02832392
		DE.CM		DE.CM-1 a DE.CM-8	RC=0,06991563
		DE.DP		DE.DP-1 a DE.DP-5	RC= 0,6117471 RC= 0,03037177
Responder		RS.RP	RC= 0,03037177	RS.RP-1	RC = 0
		RS.CO		RS.CO-1 a RS.CO-5	RC= 0,08196947
		RS.AN		RS.AN-1 a RS.AN-5	RC= 0,1009709
		RS.MI		RS.MI-1 a RS.MI-3	RC= 0,02505497
		RS.IM		RS.IM-1 a RS.IM-2	RC = 0
Recuperar		RC.RP	RC= 0,1169 RC= 0,03319449	RC.RP-1	RC = 0
		RC.IM		RC.IM-1 a RC.IM-2	RC = 0
		RC.CO		RC.CO-1 a RC.CO-3	RC = 0

6 Conclusão

A segurança cibernética é um tema ainda atual e da mais alta relevância para as sociedades contemporâneas. A seriedade com que os países mais desenvolvidos tratam o tema indica o empenho e esforço para ampliar a capacidade de atuação e a habilidade de proteger suas atividades através da rede mundial de computadores. Assim, o país precisa assumir a posição de liderança na condução da cultura de segurança cibernética entre a administração pública federal, com as mais avançadas técnicas, procedimentos e boas práticas existentes. Este trabalho, além de sugerir uma alternativa na adoção de critérios e em sua avaliação, contribui com o debate para aumentar a efetividade dos programas para a governança da segurança cibernética através de uma metodologia necessária ao seu monitoramento e avaliação.

A pesquisa foi estruturada em torno de duas questões. Primeiramente era necessário identificar que modelo conceitual e que método quantitativo de monitoramento e avaliação de sistemas de segurança da informação e cibernética deveriam ser utilizados para atender às necessidades estabelecidas pelo Decreto No 9.637. O modelo conceitual que melhor se ajusta ao problema é o CSF-NIST. Esse modelo é aplicável aos setores público e privado, devido ao seu caráter customizável, focado na melhoria da segurança e na resiliência para cada organização. Além disso, o modelo atende às necessidades mencionadas no Art. 12 e Art. 17 do Decreto No 9.637, conforme o extrato no Anexo. Sua estrutura em critérios e subcritérios é diversificada e abrangente, permitindo que todos os setores da instituição sejam avaliados, sob diferentes níveis de maturidade. A segunda questão se referia ao modo de obtenção dos pesos dos critérios e subcritérios do modelo escolhido, para monitorar e avaliar uma Instituição pública ou privada. Por se tratar de cálculo de pesos em uma estrutura hierárquica, buscou-se o método AHP, que mais se ajusta a esse tipo de problema na Pesquisa Operacional. A

quantidade e qualidade de evidências na literatura sobre o uso do AHP para a avaliação de políticas públicas corroborou a escolha por esse método.

Um estudo de caso complementou essas questões, para ilustrar como uma instituição pública ou privada pode usar o CSF-NIST com o AHP para monitorar e avaliar a maturidade da segurança da informação e cibernética em suas atividades. Assim, a estrutura do CSF-NIST foi detalhada, as etapas do AHP foram descritas, os pesos foram apresentados e, por fim, as Razões de Consistência indicaram a validação interna do processo. Em síntese, o processo de obtenção dos resultados nesta pesquisa mostrou-se mais relevante que a análise dos resultados em si, pois a maturidade de cada instituição é peculiar a cada tipo de atividade e o caso considerado está incluso nesse contexto. Assim, o objetivo geral de apoiar o processo de tomada de decisão em relação ao monitoramento e avaliação da execução da PNSI e de seus instrumentos, através de uma estrutura hierárquica e ponderada de critérios e subcritérios, elencados com base na opinião de especialistas técnicos em tecnologia da informação e usuários de sistemas informatizados, foi plenamente atendido.

A pesquisa tem, naturalmente, suas limitações. Qualquer processo de tomada de decisão com especialistas é dependente do comprometimento, da seriedade e da coerência lógica das respostas desses julgamentos. O AHP permite, de certa forma, reduzir o problema da inconsistência lógica, através do cálculo da Razão de Consistência. Entretanto, a parcialidade e efetivo conhecimento da matéria pelos especialistas consultados é algo presente e de difícil eliminação e mensuração, respectivamente. Por não se tratar de uma pesquisa com foco na qualidade dos resultados, mas no processo de obtenção dos níveis de maturidade, essa limitação não comprometeu a pesquisa. Entretanto, isto deve ser relevante para as instituições ou empresas que venham aplicar a proposta aqui desenvolvida.

Outra limitação a levantar se refere à complexidade do modelo CSF-NIST para as avaliações do AHP. A estrutura do CSF-NIST gera níveis hierárquicos com significativa quantidade de elementos, o que amplia o esforço de coleta das avaliações paritárias, gerando considerável dedicação dos especialistas para o retorno das respostas. Existem pesquisas recentes sobre a redução do esforço de coleta de dados com o AHP que podem ser aplicadas em futuras pesquisas com modelos de maturidade com tal complexidade, a exemplo do CSF-NIST. Outra possibilidade se refere à constituição de comissões de avaliação em uma instituição, com a responsabilidade e comprometimento dos agentes encarregados da tomada de decisão, na alta administração organizacional, pode contribuir para a qualidade e uniformidade das avaliações, reduzindo

o esforço individual de especialistas para a coleta dos dados. Essa medida administrativa pode ser um importante complemento ao processo desenvolvido nesta pesquisa.

Alguns aperfeiçoamentos são visualizados. A Pesquisa Operacional disponibiliza centenas de métodos de apoio à decisão multicritério que podem contribuir com o processo aqui proposto. Mesmo com a lógica do AHP, é possível, por exemplo, associar o AHP com outras técnicas ou com variáveis em lógica fuzzy. Outra possibilidade é aplicar modelos parciais do AHP, para reduzir a quantidade de avaliações, decorrentes da quantidade de variáveis a serem comparadas paritariamente.

Referências

ACZÉL, J.; SAATY, T. L. Procedures for synthesizing ratio judgements. *Journal of Mathematical Psychology*, v. 27, n. 1, p. 93–102, 1983.

AZMI, R.; TIBBEN, W.; WIN, K. T. Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, v. 3, n. 2, p. 258–283, 2018.

BADIE, N.; LASHKARI, A. H. A new evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research*, v. 2, n. 9, p. 9331–9347, 2012.

BECKER, J.; NIEHAVES, B.; POEPPELBUSS, J.; SIMONS, A. Maturity models in IS research. *In:* EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 42., 2010, Pretoria. *Anais [...]* 2010. p. 1-12.

BERNIERI, G.; DAMIANI, S.; DEL MORO, F.; FARAMONDI, L.; PASCUCCI, F.; TAMBONE, F. A Multiple-Criteria Decision Making method as support for critical infrastructure protection and Intrusion Detection System. *In*: ANNUAL CONFERENCE OF THE IEEE INDUSTRIAL ELECTRONICS SOCIETY, 2016, Florença. *Anais [...]* 2016. p. 4871–4876.

BHASKAR, S.; KUMAR, M.; PATNAIK, A. Application of Hybrid AHP-TOPSIS Technique in Analyzing Material Performance of Silicon Carbide Ceramic Particulate Reinforced AA2024 Alloy Composite. *Silicon*, p. 1–10, 2019.

BHUSHAN, N.; RAI, K. *Strategic decision making: applying the analytic hierarchy process*. London: Springer Science & Business Media, 2004.

BOWEN, P.; KISSEL, R. *NISTIR 7358: Program Review for Information Security Management Assistance (PRISMA)*. Washington, DC: [s.n.], 2007. Disponível em:

https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7358.pdf. Acesso em: 21 ago. 2020.

BRASIL. Casa Civil da Presidência da República. Instituto de Pesquisa Econômica Aplicada. *Avaliação de Políticas Públicas:* guia prático de análise Ex Ante, v.1. Brasilia-DF: Instituto de Pesquisa Econômica Aplicada. Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/180319_avaliacao_de_politicas_publicas.pdf, 2018. Acesso em: 10 jul. 2020.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa.* Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Brasilia-DF: Ministério da Defesa. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf, 2020a. Acesso em: 15 nov. 2020.

BRASIL. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. *Diário Oficial da União*: seção 1, Brasília, DF, edição 248, seção 1, p. 23, 27 dez. 2018.

BRASIL. Presidência da República. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. *Estatísticas de incidentes computacionais em órgãos de governo e vinculados – dados para diagnóstico*. Brasilia-DF: Presidência da República. Disponível em: https://www.ctir.gov.br/arquivos/estatisticas/2018/Estatisticas_CTIR_Gov_Ano_2018.pdf, 2020b. Acesso em: 10 nov. 2020.

BRASIL. Senado Federal. *Avaliação de Políticas Públicas - Resolução no 44, de 2013.* Brasilia-DF: Senado Federal. Disponível em: http://www.senado.gov.br/noticias/especiais/politicas-publicas-pnbl/Plano-de-trabalho-Avaliacao-do-PNBL-maio_2014.pdf, 2013. Acesso em: 10 nov. 2020.

BROWN, R. D. Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework. *International Review of Law*, v. 4, p. 1–35, 2018.

BUCHANAN, B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press, 2020.

CAVELTY, M. D.; BRUNNER, E. M. Introduction: Information, power, and security – An outline of debates and implications. *In:* CAVELTY, M. D.;

MAUER, V.; KRISHNA-HENSEL, S. F. *Power and Security in the Information Age:* Investigating the Role of the State in Cyberspace. Oxon: Routledge, 2007b. p. 1–18.

CESG. *Good Practice Guide (GPG40). The Information Assurance Maturity Model and Assessment Framework*. London: National Technical Authority for Information Assurance. Disponível em: https://www.ncsc.gov.uk/information/hmg-ia-maturity-model-iamm, 2015. Acesso em: 05 set. 2020.

CIS. *Center for Internet Security. About us*. New York: Center for Internet Security. Disponível em: https://www.cisecurity.org/about-us/, 2020. Acesso em: 13 out. 2020.

CURTIS, P.; MEHRAVARI, N.; STEVENS, J. *Cybersecurity Capability Maturity Model for Information Technology Services* (C2M2 for IT Services), Version 1.0. Hanscom AFB: Carnegie-Mellon Univ. Pittsburgh PA. United States. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1026943.pdf, 2015. Acesso em: 15 out. 2020.

ENGLBRECHT, L.; MEIER, S.; PERNUL, G. Towards a capability maturity model for digital forensic readiness. *Wireless Networks*, v. 26, n. 7, p. 4895–4907, 2020.

ERDOĞAN, M.; KARAŞAN, A.; KAYA, İ.; BUDAK, A.; ÇOLAK, M. A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies. *In*: INTERNATIONAL CONFERENCE ON INTELLIGENT AND FUZZY SYSTEMS. Cham: Springer, p. 1042-1049, 2019.

FORMAN, E. H. Facts and fictions about the analytic hierarchy process. *Mathematical and computer modelling*, v. 17, n. 4–5, p. 19–26, 1993.
GOIS, A. B. Segurança Cibernética. *O Comunicante*, v. 8, n. 3, p. 40–47, 2018.

HASSAN, M. H.; LEE, J. Policymakers' perspective about e-Government success using AHP approach: Policy implications towards entrenching Good Governance in Pakistan. *Transforming Government: People, Process and Policy*, v. 13, n. 1, p. 93–118, 2019.

ISA. International Society of Automation*. New ISA/IEC 62443 standard specifies security capabilities for control system components*. Disponível em: https://www.isa.org/intech/201810standards/. Acesso em: 4 nov. 2020.

ISACA. Information Systems Audit and Control Association*. COBIT - Why Cobit?* Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 2 nov. 2020.

ISO/IEC. *Information Security Management System - ISO/IEC 27000:2018*. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Acesso em: 2 nov. 2020.

ITU. *Guide to developing a National Cybersecurity Strategy - Strategic Engagement in Cybersecurity*. . Genebra: [s.n.], 2018. Disponível em: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf. Acesso em: 11 jul. 2019.

KATSIANIS, D.; NEOKOSMIDIS, I.; PASTOR, A.; JACQUIN, L.; GARDIKIS, G. Factors influencing market adoption and evolution of NFV/SDN Cybersecurity Solutions. Evidence from SHIELD Project. *In:* EUROPEAN CONFERENCE ON NETWORKS AND COMMUNICATIONS, 2018, *Anais [...]* [S.l.]: IEEE, 2018. p. 303-307.

LE, N. T.; HOANG, D. B. Can maturity models support cyber security? *In:* INTERNATIONAL PERFORMANCE COMPUTING AND COMMUNICATIONS CONFERENCE, 2016, *Anais [...]* IEEE, 2018. p. 1-7.

LIMA, P. A. L. Segurança Cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das Infraestruturas Críticas Nacionais, Órgãos Estratégicos do Governo e Forças Armadas. *In:* ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 2018, Anais *[...]* São Paulo: ABED, 2018. p. 1–24.

LIU, C. H.; LIN, C.-W. R. The Comparative of the AHP Topsis Analysis Was Applied for the Commercialization Military Aircraft Logistic Maintenance Establishment. *International Business Management*, v. 10, n. 4, p. 6428–6432, 2016.

MOMANI, A. M.; AHMED, A. A. Material handling equipment selection using hybrid Monte Carlo simulation and analytic hierarchy process. *World Academy of Science, Engineering and Technology*, v. 59, p. 953–958, 2011.

NASSER, A. A.; AL-KHULAIDI, A. A.; ALJOBER, M. N. Measuring the Information Security Maturity of Enterprises under Uncertainty Using Fuzzy AHP. *International Journal of Information Technology and Computer Science*, v. 10, n. 4, p. 10–25, 2018.

NETO, W. B. F. Cibernética como Setor Estratégico no Brasil e seus Reflexos para a Estrutura da Defesa. *Centro de Estudos Estratégicos do Exército: Análise Estratégica*, v. 17, n. 3, p. 45–64, 2020.

NIST. National Institute of Standards and Technology. *Framework for improving critical infrastructure cybersecurity, version 1.1*. Gaithersburg, MD: [s.n.], abr. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 10 nov. 2020.

NSCS. NATIONAL CYBER SECURITY CENTRE. *Cyber Assessment Framework*. . London: National Cyber Security Centre, 2018. Disponível em: https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog. Acesso em: 10 set. 2020.

PAULK, M. C.; CURTIS, B.; CHRISSIS, M. B.; WEBER, C. V. Capability Maturity Model, version 1.1. IEEE *software*, v. 10, n. 4, p. 18-27, 1993.

POMEROL, J.-C.; BARBA-ROMERO, S. *Multicriterion decision in management: principles and practice*. New York: Springer, 2012.

PÖPPELBUSS, J.; RÖGLINGER, M. What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *In:* EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 28., 2011, Helsinki. *Anais [...]* 2011. p. 1-13.

RAHIM, N. H. A.; HAMID, S.; KIAH, M. L. M.; SHAMSHIRBAND, S.; FURNELL, S. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, v. 44, n. 4, p. 606–622, abr. 2015.

RAMOS, W. M.; GOLDONI, L. R. F. Os Projetos do Exército Brasileiro e o alinhamento com as diretrizes da Estratégia Nacional de Defesa. *Revista Política Hoje*, v. 25, n. 1, p. 153–175, 2016.

REA-GUAMAN, A. M.; SÁNCHEZ-GARCÍA, I. D.; SAN FELIU GILABERT, T.; CALVO-MANZANO VILLALÓN, J. A. Modelos de Madurez en Ciberseguridad: una revisión sistemática. *In:* IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES, 28., 2017, Lisboa. *Anais [...]* 2017. p. 284-289.

SAATY, T. L. Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, v. 9, n. 3, p. 215–229, 2002.

SAATY, THOMAS L. Priority Setting in Complex Problems. *IEEE Transactions on Engineering Management*, v. EM-30, n. 3, p. 140–155, 1982.

SAATY, THOMAS L. *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980.

SAATY, T. L.; VARGAS, L. G. *Models, methods, concepts & applications of the analytic hierarchy process*. International Series in Operations Research & Management Science. New York: Springer Science & Business Media, v. 175, 2012.

STERLING, B. *The hacker crackdown:* Law and disorder on the electronic frontier. [S.l.]: Open Road Media, 2020.

SYAMSUDDIN, I. Multicriteria Evaluation and Sensitivity Analysis on Information Security. *International Journal of Computer Applications*, v. 69, n. 24, p. 22–25, 2013.

SYMANTEC. *Cyber Security Insights Report - Global Results*. . [S.l: s.n.], 2018. Disponível em: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2017-ncsir-global-results-en.pdf. Acesso em: 10 nov. 2020.

TEICHERT, R. Digital transformation maturity: A systematic review of literature. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis,* v. 67, n. 6, p. 1673-1687, 2019.

VARGAS, L. G. Reciprocal matrices with random coefficients. *Mathematical modelling*, v. 3, n. 1, p. 69–81, 1982.

VIANNA, E. W.; DE SOUSA, R. T. B. Ciber Proteção: a segurança dos sistemas de informação no espaço cibernético. *Revista Ibero-Americana de Ciência da Informação*, v. 10, p. 110–131, 2018.

WHITE, G. *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Global*. Chicago: Reaktion Books, 2020.

WIND, Y.; SAATY, T. L. Marketing Applications of the Analytic Hierarchy Process. *Management Science*, v. 26, n. 7, p. 641–658, 1980.

YUEN, K. K. F. Towards a Cybersecurity Investment Assessment method using Primitive Cognitive Network Process. *In:* INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE IN INFORMATION AND COMMUNICATION, 2019, *Anais [...]* 2019. p. 68–71.