CLEITON ALMEIDA ATAIDE

ANÁLISE DO ESTABELECIMENTO DO PROCESSO DE DECISÃO COLABORATIVA PARA A GOVERNANÇA DE CIBERSEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Coronel R1 João de Azevedo

Rio de Janeiro
2023

RESUMO

No nosso mundo atual, estamos cercados de computadores e dispositivos que facilitam a nossa vida. Esta constatação também é verdadeira no âmbito tanto das organizações quanto dos governos e países. Essa grande quantidade de serviços digitais aumenta significativamente a chamada superfície de ataque, isto é, aumenta a quantidade de locais e formas de ataques possíveis em nosso ambiente cibernético. A possibilidade de um ataque a uma infraestrutura crítica do país é real. Este trabalho é um ensaio acadêmico que aborda a aplicação da colaboração na tomada de decisões em cibersegurança, especialmente no contexto de infraestruturas críticas, relacionando conceitos como decisão colaborativa e governança de cibersegurança, avaliando o estabelecimento de um processo de decisão colaborativa para a gestão de infraestruturas críticas. O trabalho começa com uma introdução e, em seguida, apresenta os conceitos de processo de decisão colaborativa, governança de cibersegurança e cibersegurança de infraestruturas críticas. Também são discutidos os principais pontos de uma boa governança de cibersegurança de infraestruturas críticas e a aplicação da decisão colaborativa neste contexto. Ao final são apresentadas algumas considerações finais e recomendações de continuação do trabalho.

Palavras–chave: cibersegurança de infraestrutura crítica; decisão colaborativa; governança cibernética; governança de cibersegurança; infraestruturas críticas.

ABSTRACT

Nowadays, we are surrounded by computers and devices that make our lives easier. This finding is also factual within the environment of organizations, governments, and countries. This large number of digital services significantly increases the so-called attack surface, i.e., it increases the number of locations and ways of possible attacks in our cyber environment. The possibility of an attack on the country's critical infrastructure is real. This work addresses the importance of collaboration in decision-making in cybersecurity, especially in the context of critical infrastructures, correlating concepts such as collaborative decision-making and cybersecurity governance and evaluating the establishment of a collaborative decision-making process for infrastructure management criticism. The work begins with an introduction and then presents the concepts of collaborative decision-making, cybersecurity governance, and cybersecurity of critical infrastructures. The main challenges in the cybersecurity governance of critical infrastructures and applying a collaborative decision process in managing these infrastructures are also considered. Lastly, some final considerations and recommendations for continuing the work are presented.

Keywords*: critical infrastructure cybersecurity; collaborative decision making; cyber governance; cybersecurity governance; critical infrastructure.*

SUMÁRIO

1 INTRODUÇÃO

No nosso mundo atual, estamos cercados de computadores e dispositivos que facilitam a nossa vida. Esta constatação também é verdadeira no âmbito tanto das organizações quanto dos governos e países. Especialmente no Brasil, o governo federal disponibiliza muitos serviços digitais para a nossa população, sendo considerado um dos mais digitais do mundo, como mostra o relatório do Banco Mundial (World Bank, 2022). Essa grande quantidade de serviços digitais aumenta significativamente a chamada superfície de ataque, isto é, aumenta a quantidade de locais e formas de ataques possíveis em nosso ambiente cibernético. A possibilidade de um ataque a uma infraestrutura crítica do país é real e de acordo com relatório do Fórum Econômico Mundial, o risco de um ataque cibernético grave nos próximos cinco anos está entre os dez maiores (World Economic Forum, 2023).

Desde a aprovação da Estratégia Nacional de Defesa em 2008 (Brasil, 2008) o Brasil reconheceu o setor cibernético como estratégico para o país e para a salvaguarda das infraestruturas críticas (IC) para o pleno funcionamento do Estado brasileiro. Mais recentemente, foi aprovado o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) estabelecendo oito áreas como críticas: águas, energia, transporte, comunicações, finanças, biossegurança e bioproteção e defesa (Brasil, 2022). O PLANSIC trata de forma integrada as IC e embora não seja restrito a área cibernética, esta vem inegavelmente ganhando mais relevância no contexto de segurança dessas infraestruturas.

Com a implementação do Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, será possível o acompanhamento e monitoramento permanente dessas IC (Brasil, 2022). Tendo em vista que um dos principais riscos advém do domínio cibernético, faz-se necessário o estabelecimento de um processo de governança adequado para coordenações de ações, sobretudo em momentos de crise. Esse processo precisa levar em consideração a interdependência das IC, seus diferentes níveis de maturidade no campo cibernético, os impactos na tomada da decisão de qual ação priorizar e qual efeito indesejável seria melhor evitar.

Neste sentido, o presente trabalho busca contribuir com a problemática descrita anteriormente, analisando a adoção do processo de decisão colaborativa dentro de um gabinete de crises, ou sala de comando e controle das nossas infraestruturas

críticas nacionais. Contudo, não possui como objetivo a obtenção de conclusões definitivas. Por por se tratar de um Ensaio Acadêmico, o objetivo foi, portanto, apenas correlacionar alguns conceitos como os de decisão colaborativa, governança de cibersegurança aplicadas no contexto de cibersegurança de infraestruturas críticas, avaliando-se o estabelecimento de um processo de decisão colaborativa nesse contexto.

Com o objetivo descrito anteriormente, o trabalho foi dividido em seis capítulos, sendo o primeiro a introdução e o sexto o das considerações finais. No capítulo 2 são apresentados alguns fundamentos relativos ao processo de decisão colaborativa. No capítulo 3 o tema de governança de cibersegurança é discutido brevemente, sendo acrescentado alguns aspectos de cibersegurança de infraestruturas críticas no capítulo 4. Já no capítulo 5 é feita uma breve análise conjunta de todos os conceitos com as conclusões sendo sumarizadas no capítulo de considerações finais. Por fim, apresentamos todas as referências utilizadas na construção do trabalho.

2 PROCESSO DE DECISÃO COLABORATIVA

O processo de decisão colaborativa tem sido aplicado em diversos contextos, como gerenciamento de tráfego aéreo (Ball, *et al.*, 2008); saúde (Trede; Higgs, 2008); gerenciamento de emergências (Kapucu; Garayev, 2011); etc.

Segundo Owen (2015), o processo de decisão colaborativa é um processo no qual são agregadas as percepções dos múltiplos decisores numa alternativa mais significativa para todos, do que as várias alternativas de cada decisor isoladamente, sendo esta uma escolha do grupo e não de uma pessoa isoladamente, todos se sentem donos facilitando a sua implementação.

Um arcabouço teórico para esse tipo de agregação foi proposto por Keeney (2013), no qual ele parte da análise da decisão individual e apresenta uma forma possível de agregação por meio do seu teorema da análise da decisão em grupo, que consiste em encontrar uma função utilidade para o grupo a partir das funções utilidade individuais, sendo a função utilidade para o grupo uma soma ponderada das funções utilidade individuais. Um dos seus pontos fortes é a consistência, a qual foi incorporada no modelo por meio dos princípios de comportamento cosistentente e princípios de atribuição de pesos para dimensionar preferências por consequências e julgamentos relativos a eventos.

Já a modelagem apresentada por Owen (2015) sugere algumas modificações no processo de análise da decisão colaborativa divididas em quatro fases: estrutura colaborativa; alternativas colaborativas; entendimento colaborativo e conexão colaborativa, as quais são discutidas com poucos detalhes a seguir.

2.1 Estrutura de Colaboração

Segundo Owen (2015), a Estrutura de Colaboração é aquela aceita por todos os decisores individuais após o processo de agregação. Neste sentido, é assumido que o grupo terá uma visão mais completa do problema da decisão do que qualquer visão individual de um decisor.

A Estrutura de Colaboração é desenvolvida na fase de estruturação do processo colaborativo de tomada de decisão e envolve compartilhar informações, discutir diferentes perspectivas e trabalhar em conjunto para desenvolver uma compreensão compartilhada do problema de decisão.

Os resultados específicos desta fase são uma hierarquia de decisão e um diagrama de relevância que todos os participantes concordam que descrevem a decisão a ser tomada. A hierarquia de decisão identifica as principais decisões a serem tomadas, enquanto o diagrama de relevância identifica os atributos de valor que são importantes para a decisão.

2.2 Alternativas Colaborativas

A segunda fase do modelo de Owen (2015) é a das Alternativas Colaborativas, cujo objetivo é desenvolver de três a cinco alternativas que abranjam todo o espaço das alternativas colaborativas, dentro da estrutura de colaboração montada para o problema de decisão em questão.

Em grupo e utilizando-se de processos como *brainstorming* um grupo mais amplo de alternativas podem ser identificadas e avaliadas quanto a viabilidade, efetividade e alinhamento com respeito aos valores e objetivos e metas traçadas para o grupo de decisores.

Assim, a alternativa que representa a melhor estratégia pode mais adiante ser escolhida pelo grupo como sendo aquela cujo entendimento comum concorda como sendo a melhor dentre todas possíveis levantadas.

2.3 Entendimento Colaborativo

A terceira fase no modelo de Owen (2015) é a do Entendimento Colaborativo, a qual consiste na construção de uma visão compartilhada entre os decisores sobre os pontos positivos e negativos, fontes de valor e riscos associados a cada uma das alternativas da fase anterior.

Esta fase envolve a colaboração, cogitação e diálogo por meio dos quais se constrói uma compreensão conjunta, não se tratando, portanto, da seleção de uma alternativa.

2.4 Conexão Colaborativa

A última fase do modelo de Owen (2015) é a da Conexão Colaborativa na qual se desenvolve uma estratégia híbrida nova e de maior valor que as que estão de posse do grupo de decisores.

Uma estratégia híbrida é uma nova estratégia, a qual combina de forma coerente os componentes de maior valor de cada uma das alternativas inicialmente definidas. Nela o grupo trabalha em conjunto desenvolvendo explicações convincentes para o compromisso de todos com a nova estratégia.

Esta fase é importante, pois ajuda a garantir que a decisão seja baseada em uma avaliação minuciosa de todas as opções possíveis e alinhadas com os valores e objetivos traçados pelo grupo de decisores inicialmente.

No processo de decisão colaborativa toma-se crédito de que cada decisor tem um entendimento incompleto (visão, estrutura, informação e valores) de como o mundo funciona, isto é, de certa forma a visão de cada decisor individualmente possui uma maior incerteza daquela obtida colaborativamente.

Este processo, se mostra flexível, haja visto sua utilização em vários contextos. Um bom exemplo pode ser encontrado nos casos ligados ao controle de tráfego aéreo

e administração de aeroportos (Ribeiro, 2013), nestes casos o processo de decisão colaborativa já vêm sendo estudados e aplicados sistematicamente, inclusive com o desenvolvimento de ferramentas automáticas de auxílio à decisão (Zaraté, 2013).

O processo de análise da decisão colaborativa agrega o entendimento dos decisores individuais por meio de análise construindo um entendimento mais completo do mundo por meio de um pensamento coletivo.

Contudo, outros fatores pertinentes às dinâmicas de grupos, como ambientes muito competitivos, podem gerar conflitos internos, os quais podem atrapalhar a eficiência do processo (Gençer, 2019).

Em seguida serão apresentados algumas características necessárias ao processo de governança de cibersegurança.

3 GOVERNANÇA DE CIBERSEGURANÇA

Não há dúvidas da importância que o espaço cibernético tem hoje na vida das pessoas, das empresas, dos governos e países. O nível de dependência das tecnologias digitais nos dias atuais tem imposto riscos cada vez mais crescentes quanto à segurança no ambiente cibernético. Assim, surgiu naturalmente a necessidade de definição cibersegurança como sendo: a coleção de ferramentas, políticas, conceitos relativos a segurança, salvaguardas, diretrizes, formas de gerenciamento de risco, ações, treinamentos, melhores práticas, garantias e tecnologias, as quais podem ser usadas na proteção do ambiente cibernético da organização, seus ativos e usuários ITU (2008, p. 2).

No âmbito das organizações surge então a necessidade de estabelecer dentro dos processos de governança, algumas particularidades que sejam capazes de lidar com as questões introduzidas pelo conceito de cibersegurança e afetam os negócios, planejamentos estratégicos, a credibilidade de empresas, organizações e países. Assim, a governança cibernética pode ser entendida como sendo a operação de processos de tomada de decisão de forma a enfatizar a participação, a transparência e a responsabilização de medidas relacionadas com o ciberespaço, conjuntamente com mecanismos advindos de acordos internacionais, de estratégias, leis, de medidas, de regulamentos e padrões, sendo tudo interligado de maneira eficiente (Savaş; Karataş, 2022).

Dentro deste espectro amplo de governança cibernética, podemos definir a governança de cibersegurança como o processo de gerenciamento e proteção de ativos de informação e tecnologia contra as ameaças cibernéticas e compreende a implementação de políticas, procedimentos e controles de forma a garantir a confidencialidade, a integridades e a disponibilidade de informações, dados e dispositivos (Savaş; Karataş, 2022).

O estudo mencionado anteriormente comparou diversos trabalhos sobre os temas de governança cibernética e governança de cibersegurança e sugere que um *framework* aplicável para uma boa governança de cibersegurança precisa:

- **Possuir validade geral**: as políticas determinadas devem ser válidas para todas as instituições, indivíduos e dispositivos em ambientes cibernéticos;
- **Ser reconhecida internacionalmente**: deve ser um tipo de política que todos os estados aceitem e implementem, e não um ou alguns;
- **Ser adaptável:** as políticas determinadas devem ser adaptáveis às questões de subdomínios dos ambientes cibernéticos (por exemplo, cibersegurança, computação em nuvem, IoT, etc.). O número de componentes em ambientes cibernéticos cresce continuamente e, portanto, novas áreas de subconjuntos estão constantemente sendo formadas;
- **Ser participativa**: é necessário considerar participantes que representem todos os setores público, privado e usuários individuais nas políticas a serem determinadas;
- **Ser inclusiva**: as políticas determinadas devem abranger todas as instituições, organizações e usuários – e não um único grupo;
- **Ser desenvolvível**: a governança de cibersegurança deve ser capaz de se adaptar a situações em mudança advindas do desenvolvimento da tecnologia.
- **Ser vinculativa**: a governança de cibersegurança deve ser vinculativa para todos os elementos que se utilizam de ambientes cibernéticos e deve ser capaz de impor sanções.

Um outra perspectiva de governança de cibersegurança apresentada é que para ser efetiva, uma governança de cibersegurança precisa abordar conceitos como estratégia de cibersegurança e objetivos; processos padronizados; conformidade, sanções e responsabilização; supervisão da liderança sênior; e recursos (Savaş; Karataş, 2022). Os processos padronizados precisam estar integrados aos sistemas e processos já existentes dentro da agenda de gerenciamento das lideranças. As

estratégias de cibersegurança devem ser construídas com a premissa de resiliência e defesa ativa considerando tanto as tecnologias quanto os fatores humanos. O papel da liderança na supervisão é crucial para que a governança seja efetiva, assim como para a consciência situacional de cibersegurança, educação e treinamento, os quais devem ser baseados em melhores práticas.

4 CIBERSEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Em 2018 o *National Institute of Standards and Technology* (NIST) atualizou o seu *framework* para a melhoria da cibersegurança de infraestruturas críticas (Barrett, 2018), o qual é baseado no gerenciamento de riscos, propondo uma maneira de gerenciá-los e reduzi-los. Esse *framework* é composto de três partes: o núcleo central; os níveis de implementação e os perfis, sendo que em cada parte são reforçados os aspectos do negócio e a missão da organização nas atividades de segurança cibernética, conforme detalhado abaixo.

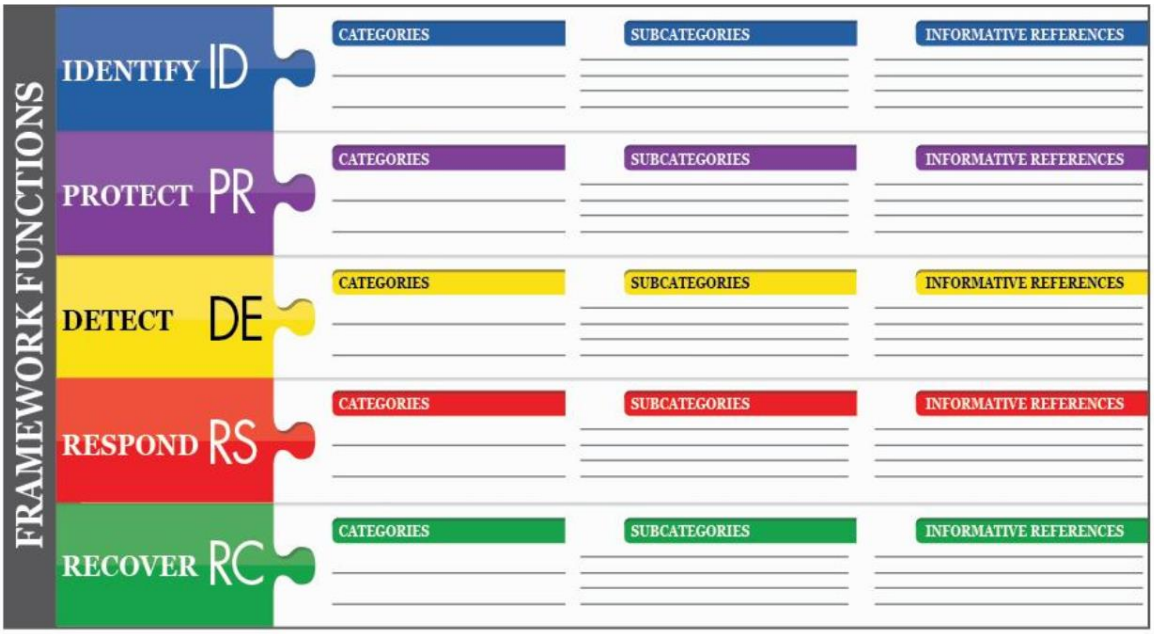
4.1 Núcleo Central

O Núcleo Central do *framework* proposto pelo NIST, representa um conjunto de atividades de cibersegurança, resultados desejados e referências aplicáveis, os quais podem ser aplicados comumente às infraestruturas críticas e é composto por funções, categorias, subcategorias e referências informativas.

As **Funções** são em número de cinco (Identificar, Proteger, Detectar, Responder e Recuperar) e organizam as atividades de cibersegurança no seu mais alto nível, ajudando as organizações a executar o seu gerenciamento e decisões relativas aos riscos à segurança cibernética, tratamento de ameaças e melhorias, por meio do aprendizado obtido de atividades anteriormente realizadas, isto é, propiciam uma evolução. Além disso, as **Funções** estão alinhadas com metodologias de gerenciamento de incidentes e evidenciam os impactos dos investimentos da organização em cibersegurança.

Já as **Categorias** são divisões de cada Função em grupos de entregáveis relativos à cibersegurança intimamente ligados às necessidades programáticas e atividades específicas. Exemplos de **Categorias** dentro da função Identificar incluem o "gerenciamento de ativos", na função Detectar incluem o "processo de detecção".

Figura 1 - Descrição do Núcleo Central do *framework*



Fonte: Barrett, 2018, p. 6

Por sua vez, as **Subcategorias**, como o nome sugere, são subdivisões das Categorias em entregáveis resultantes de atividades técnicas ou gerenciais. Elas fornecem um conjunto de resultados, ainda que não exaustivos, os quais suportam a obtenção de resultados específicos em cada Categoria. Como exemplos de **Subcategorias** podem ser 'sistemas de informações externas estão catalogados', 'dados em repouso estão protegidos' ou 'notificações de sistemas de detecção são investigadas'.

Além disso, as Referências Informativas são trechos específicos de padrões, guias e melhores práticas comuns aos setores de infraestruturas críticas que servem de referência e ilustram como os resultados associados a cada Subcategoria podem ser obtidos.

4.2 Níveis de Implementação (*Tiers*)

Os Níveis de Implementação fornecem às organizações uma maneira de avaliar suas práticas atuais em cibersegurança e determinar o estado do gerenciamento do risco à segurança cibernética desejado. Por meio dos Níveis, as

organizações estabelecem um caminho a ser seguido para alcançar os objetivos de cibersegurança.

Os níveis vão de Parcial (nível 1) até Adaptativo (nível 4) e estão baseados nas práticas de gerenciamento de riscos, no ambiente de ameaças, nos requisitos de legislação e outras restrições organizacionais. Em seguida são apresentados mais detalhes sobre os quatro níveis.

- **Parcial** (Nível 1): As organizações neste nível possuem um processo *ad hoc* para o gerenciamento de riscos afetos à cibersegurança. Elas apresentam algumas práticas de cibersegurança, contudo essas práticas não estão integradas aos processos de gerenciamento de riscos geral da organização.
- **Risco Informado** (Nível 2)**:** As organizações neste nível já possuem um processo de gerenciamento de risco afetos à cibersegurança formalizado. Elas apresentam processo para identificação, avaliação e gerenciamento desses riscos, porém sem estarem integrados aos processos de gerenciamento de riscos geral da organização.
- **Repetível** (Nível 3): As organizações possuem processos padronizados para gerenciamento de riscos afetos a cibersegurança, os quais foram integrados aos processos gerais de gerenciamento de riscos. Além disso, regularmente implementam processos de avaliação e melhoria das práticas em cibersegurança, apresentando, também, políticas e procedimentos para resposta a incidentes de cibersegurança.
- **Adaptativo** (Nível 4): Neste nível, as organizações possuem uma maneira ágil e proativa no gerenciamento de riscos afetos a cibersegurança, sendo capazes de rapidamente se adaptarem às mudanças no seu ambiente de riscos. Possuem também processos de melhoria contínua para suas atividades relacionadas com cibersegurança, com estabelecimento de métricas para a medida efetiva de suas práticas e com o uso dessas métricas estabelecem suas decisões.

4.3 Perfis

Com o *framework* desenvolvido pelo NIST se pode levantar o Perfil atual da organização, que pode ser utilizado na construção de uma caminho a ser seguido para

a melhoria das práticas de gerenciamento de riscos afetos à cibersegurança. O Perfil nada mais é do que o alinhamento entre as Funções, Categoria e Subcategorias com os requisitos de negócio e tolerância a risco da organização e ajuda a comunicar a percepção de risco aos *stakeholders.*

Os Perfis podem ser utilizados para descrever o estado atual de uma atividade. Assim, o Perfil Atual indica os resultados de cibersegurança que estão sendo atingidos no momento, enquanto o Perfil Desejado indica os resultados almejados para gerenciamento de riscos. A comparação entre o Perfil Atual e o Desejado pode servir para elaboração de planos de ação para a diminuição da diferença entre as Categorias e Subcategorias associadas a cada Perfil estabelecendo um caminho a ser seguido pela organização.

Nosso objetivo neste capítulo não é aprofundar no tema, mas sim apresentar uma breve visão do *framework* sobre melhoria da cibersegurança de infraestruturas críticas, maiores detalhes podem ser encontrados em (Barrett, 2018).

5 DECISÃO COLABORATIVA E GESTÃO DE INFRAESTRUTURAS CRÍTICAS

O Brasil aguarda a criação de uma Agência Nacional de Cibersegurança (ANCiber) por meio da publicação da Política Nacional de Cibersegurança (Brasil, 2023). Dentro do escopo de trabalho da nova Agência está prevista a criação de um gabinete de crises de incidentes cibernéticos, no qual poder-se-ia instalar um processo de decisão colaborativa. Idealmente, este gabinete poderia estar sempre ativado e monitorando as principais infraestruturas críticas do país e passando a gabinete de crise, conforme fosse necessário.

Um exemplo de funcionamento de uma estrutura permanente que utiliza-se de um processo de decisão colaborativa é o Centro de Gestão da Navegação Aérea (CGNA), órgão subordinado ao Departamento de Controle do Espaço Aéreo (DECEA) responsável pelo gerenciamento de fluxo das aeronaves que circulam no Brasil e que em caso de necessidade, por exemplo, o fechamento de um aeroporto toma decisão de forma colaborativa com as concessionárias e linhas áereas da melhor decisão a ser tomada para minimizar os impactos desse fechamento para os passageiros em voo e no solo e demais interessados (Brasil, 2018).

As infraestruturas críticas são nacionais são caracterizadas por apresentarem diferentes níveis de maturidade em cibersegurança. Isto é, sendo importante que se leve este fator na tomada de decisão pois deveremos encontrar organizações que se enquadram nos diferentes níveis (N1 a N4) de implementação, conforme apresentado na seção 4.2.

Assim, um plano poderia ser estabelecido com base nos níveis e diferentes perfis atuais, com o estabelecimento de um perfil e/ou nível desejado a ser alcançado, podendo essa evolução ser acompanhada e os principais riscos monitorados pela nova Agência.

Analisando agora os requisitos apontados em Savas e Kratas (2022) para que uma governança de cibersegurança, pode-se notar que muitos deles são compatíveis com a proposta de um gabinete de crises com um processo colaborativo de tomada de decisão, pois os quesitos de ser participativo, inclusivo e adaptável são inerentes ao processo de decisão colaborativa.

Como mencionado no capítulo 2 a decisão colaborativa já vem sendo utilizado em muitos contextos diferentes, e sendo usado internacionalmente no setor de tráfego aéreo, inclusive no Brasil, conforme mencionado anteriormente. Existe uma recomendação feita pela Organização da Aviação Civil Internacional (ICAO) que estabelece como implementar o processo de decisão colaborativa nos principais aeroportos do mundo (International Civil Aviation Organization, 2018). Assim, pode-se confirmar o caráter internacional do processo.

Outro fator de destaque do processo de CDM seria a possibilidade dele ser possível de ser automatizável em alguma medida com o uso de ferramentas conforme já vem sendo feito em outros contextos (Zaraté, 2013). Com a utilização de ferramentas de monitoramento contínuo, como indicadores chave de performance, um processo de CDM pode ser instrumentalizado e evoluído.

Ainda segundo Savas e Kratas (2022), a governança precisa possuir caráter geral e vinculativa, isto é, devendo ser possível a autoridade competente a possibilidade de aplicações de sanções em caso de inobservância das políticas e procedimentos estabelecidos, fato esse que já faz parte do caráter regulador e fiscalizador de uma Agência Reguladora, como é o caso da ANCiber.

Desta forma, após as análises realizadas anteriormente, fica evidente que um processo de decisão colaborativa para a governança de cibersegurança em

infraestruturas críticas pode ser aplicado pois possui todos os requisitos que possibilitam uma boa governança.

Por questões de limitação de escopo e de tempo, o processo de como isso poderia ser implementado não será desenvolvido aqui. Ficando com sugestão para trabalhos posteriores a questão de como implementá-lo e a avaliação pós implementação.

Contudo, uma sugestão seria realizar uma pesquisa de campo para tentar capturar as percepções de pessoas que atuam em lugares que possuem este processo implementado, como CGNA aqui no Brasil. Bem como, a percepção também de pessoas que atuam em locais que trabalham com a segurança cibernética e com infraestruturas críticas.

6 CONSIDERAÇÕES FINAIS

Atualmente, estamos cercados por computadores e dispositivos que tem facilitado a nossa vida, a vida de nossas empresas e governos. Esta grande exposição ao ambiente cibernético tem levado ao aumento de incidentes cibernéticos ao redor do mundo. O relatório de riscos do Fórum Econômico Mundial têm apontado, mais recentemente, o risco de um evento cibernético grave como um dos dez mais prováveis (World Economic Forum, 2023).

No Brasil, o setor cibernético passou a ser considerado estratégico após aprovação da Estratégia Nacional de Defesa (Brasil, 2008) e com a grande quantidade de serviços digitais oferecidos pelo Governo Federal, o país possui hoje uma elevada superfície de ataque. Por isso mesmo, a possibilidade de ataque cibernético a uma infraestrutura crítica é real.

Essa condição tem levado o Estado Brasileiro a se estruturar com a publicação da PLANSIC (Brasil, 2022) e recentemente a promessa de criação de uma Agência reguladora de cibersegurança.

O presente trabalho, procurou analisar a problemática da governança de cibersegurança de infraestruturas críticas e a possível criação de um gabinete de crise de eventos cibernéticos que implementasse um processo de decisão colaborativa para tomada de decisão sobre as ações a serem tomadas, prioridades a serem observadas, os efeitos adversos a serem evitados.

No capítulo 2, foram apresentados os conceitos que estão relacionados ao processo de decisão colaborativa, o qual possui a característica de possuir uma qualidade final da decisão superior ao dos diversos decisores individuais isoladamente. Além disso, a decisão possui uma aceitação maior por parte de todos, pois ela é de todos.

No capítulo 3 foi apresentado os resultados de um estudo comparativo de diversos trabalhos sobre os temas de governança cibernética e governança de cibersegurança no qual é sugerido alguns atributos (sete atributos) que um framework de governança de cibersegurança precisa possuir para ser eficaz (Savaş; Karataş, 2022).

O capítulo 4 procurou apresentar um framework do NIST que trata de cibersegurança de infraestruturas críticas, que é composto por três partes: Núcleo Central, Níveis de Implementação e Perfis. Este *framework* pode ser usado para diagnóstico e planejamento para evolução dos níveis de segurança cibernética das infraestruturas críticas.

Após as análises preliminares sobre a adequação e viabilidade de se implementar o processo de decisão colaborativa para a governança de cibersegurança de infraestruturas críticas apresentadas no capítulo 5, pode-se concluir inicialmente que o processo possui os requisitos sugeridos por Savas e Kratas (2022) e por conseguinte possibilitando o ganho no resultado final das decisões de um eventual gabinete de crise de eventos cibernéticos.

Cabe mencionar que os resultados de melhores decisões de grupo estão sujeitos também a possíveis conflitos internos que podem corroer os avanços prometidos (Gençer, 2019). Portanto, isto deve ser levado em consideração quando da escolha dos representantes escolhidos para o grupo de decisores.

Como mencionado, este trabalho é apenas um trabalho preliminar e como continuidade para aprofundamento, sugere-se realizar uma pesquisa de campo para tentar capturar as percepções de pessoas que atuam em lugares que possuem este processo implementado, como CGNA aqui no Brasil. Bem como, a percepção também de pessoas que atuam em locais que trabalham com a segurança cibernética e com infraestruturas críticas.

REFERÊNCIAS

BALL, Michael O. *et al*. **Collaborative decision making in air traffic management: Current and future research directions**. Springer Berlin Heidelberg, 2001.

BARRETT, Matthew. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. [*S. l.*]: **NIST Cybersecurity Framework**, 2018.

BRASIL. Comando da Aeronáutica. Portaria DECEA nº136/DGCEA, de 4 de setembro de 2018. Aprova a reedição da Instrução que trata do Serviço de Gerenciamento de Fluxo de Tráfego Aéreo (ICA 100-22). **Boletim do Comando da Aeronáutica**: n. 159, 11 set. 2018.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa e dá outras providências. Brasília, DF: Presidência da República, [2008]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 30 out. 2023.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em: 30 out. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **GSI/PR realiza Audiência Pública para discutir criação da Política Nacional de Cibersegurança (PNCiber)**: a ideia é centralizar a segurança cibernética na estrutura do governo federal. Brasília, DF: GSI, 2023. Disponível em: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/gsi-realiza-audiencia-publica-para-discutir-criacao-da-politica-nacional-de-ciberseguranca-pnciber-1. Acesso em: 30 out. 2023.

GENÇER, Hüseyin. Group Dynamics and Behaviour. **Universal Journal of Educational Research**, v. 7, n. 1, p. 223-229, 2019. DOI 10.13189/ujer.2019.070128.

INTERNATIONAL CIVIL AVIATION ORGANIZATION. **DOC 9971 - Manual on Collaborative Air Traffic Flow Management (ATFM)**. 3rd ed. Montreal: ICAO, [2018].

INTERNATIONAL TELECOMMUNICATION UNION. Standardization of Sector:; ITU-Tx. 1205. **Interfaces**, v. 10, n. 20-X, p. 49, 2008.

KAPUCU, Naim; GARAYEV, Vener. Collaborative decision-making in emergency and disaster management. **International Journal of Public Administration**, v. 34, n. 6, p. 366-375, 2011. DOI 10.1080/01900692.2011.561477.

KEENEY, Ralph L. Foundations for group decision analysis. **Decision Analysis**, v. 10, n. 2, p. 103-120, 2013. DOI https://doi.org/10.1287/deca.2013.0265.

OWEN, Daniel. Collaborative decision making. **Decision Analysis**, v. 12, n. 1, p. 29-45, 2015. DOI https://doi.org/10.1287/deca.2014.0307.

RIBEIRO, Vitor Filincowsky. Decisão colaborativa com utilização de Teoria dos Jogos para o sequenciamento de partidas em aeroportos. 2013.

SAVAŞ, Serkan; KARATAŞ, Süleyman. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. **International Cybersecurity Law Review**, v. 3, n. 1, p. 7-34, 2022.

TREDE, Franziska; HIGGS, Joy. Collaborative decision making. **Clinical reasoning in the health professions**, p. 43-54, 2008.

WORLD BANK. **GovTech Maturity Index, 2022 Update**: trends in public sector digital transformation. [*S. l.*]: World Bank Group, 2023. Disponível em: https://doi.org/10.1596/38499. Acesso em: 30 out. 2023.

WORLD ECONOMIC FORUM. **The Global Risk Report.** 18th ed. Insight Report. [*S. l.*]: WEF, 2023. Disponível em: https://www3.weforum.org/docs/WEF_Global _Risks_Report_2023.pdf. Acesso em: 30 out. 2023.

YUSIF, Salifu; HAFEEZ-BAIG, Abdul. A conceptual model for cybersecurity governance. **Journal of Applied Security Research**, v. 16, n. 4, p. 490–513, 2021. Disponível em: https://doi.org/10.1080/19361610.2021.1918995. Acesso em: 30 out. 2023.

ZARATÉ, Pascale. **Tools for collaborative decision-making**. [*S. l.*]: John Wiley & Sons, 2013.