risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 09/05/2022
Aceitação/Acceptance: 29/07/2022

Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação

Marcus Aurélio Carvalho Georg[1], Walisson Magno Silva Rodrigues[2], Carlos André de Melo Alves[2], Aldery Silveira Júnior[2], Rafael Rabelo Nunes[1,2,3]

georg@stj.jus.br; walissonmagnos@gmail.com; carlosandre@unb.br; aldery@unb.br; rafaelrabelo@unb.br.

[1] Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - Zipcode 70297-400.

[2] Universidade de Brasília, Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE, Departamento de Administração, Brasília, Brasil - Zipcode 70910-900.

[3] Centro Universitário UniAtenas, Paracatu-MG, Brasil – Zipcode 38602-108.

Pages: 602-616

Resumo: A Segurança Cibernética vem ganhando papel de destaque e mostrando-se imprescindível para os avanços na transformação digital brasileira, inclusive no setor público. O objetivo desse trabalho foi mapear os principais desafios da segurança cibernética no setor público federal do Brasil sob a ótica de gestores de tecnologia da informação (TI). Para isso, foram realizadas entrevistas semiestruturadas com gestores de TI que atuam na área de segurança cibernética dos três poderes da república (executivo, legislativo e judiciário). As entrevistas foram transcritas e analisadas pela técnica de análise de conteúdo para formar construtos que representassem os principais desafios relatados na ótica dos entrevistados. A partir do resultado, identificou-se nove construtos que representam os desafios e, consequentemente, pontos de atenção para os gestores de segurança cibernética no setor público federal brasileiro. Este trabalho contribui para estudos relativos a adoção da segurança cibernética na área pública.

Palavras-chave: segurança cibernética; tecnologia da informação; setor público; segurança da informação.

The challenges of Cybersecurity in the federal public sector in Brazil: a study from the perspective of information technology managers

Abstract: Cybersecurity has been gaining a prominent role and proving to be essential for advances in Brazilian digital transformation, including in the public sector. The objective of this work was to map the main challenges of cybersecurity in the federal public sector in Brazil from the perspective of information technology managers. For this, semi-structured interviews were carried out with information technology managers who work in the cyber security area of the three powers of

the republic (executive, legislative and judicial). Many challenges reported from the perspective of the interviewees. From the result, nine constructs were identified that represent the challenges and, consequently, points of attention for cybersecurity managers in the Brazilian federal public sector. This work contributes to studies related to the adoption of cyber security in the public area.

Keywords: cybersecurity; information technology; public sector; information security.

1. Introdução

A evolução das atividades cibernéticas maliciosas aumentou os riscos cibernéticos para os indivíduos, organizações e governos, tornando a Segurança Cibernética (SC) uma temática essencial das decisões sociais, políticas e econômicas (Geer et al., 2020). Trata-se de um tema complexo e relevante, sendo seu conhecimento essencial para pessoas e organizações, abrangendo uma gama de aspectos técnicos, organizacionais e de governança que devem ser considerados para proteger os sistemas de informação contra ameaças acidentais e deliberadas. Isso vai muito além dos pormenores da criptografia, firewalls, software antivírus, e ferramentas técnicas de segurança similares (Veale & Brown, 2020).

O desafio está em sair das soluções tradicionais, focadas na resiliência, para programas nacionais, patrocinados pelos maiores interessados. A exemplo disso, EUA, Holanda, Alemanha e Reino Unido introduziram estratégias nacionais de segurança cibernética, assim como a União Europeia (UE), Organização das Nações Unidas (ONU) e a Organização do Tratado do Atlântico Norte (OTAN) desenvolvem políticas internacionais com foco na resiliência a desastres, devendo, em seguida, de forma estratégica, seguir do "o que fazer" para o "como fazer" (Sharkov, 2016).

As organizações precisam intensificar seus mecanismos de segurança, criando regras e políticas para seus usuários, que lhes permitam proteger seus sistemas e dados (Costa et al., 2019). No setor público brasileiro não foi diferente, desafios complexos relacionados à SC e as rápidas transformações na economia e na sociedade, proporcionadas pelo ambiente digital, impuseram novas ações e estratégias no setor público federal brasileiro (Brasil, 2018), haja vista o quantitativo de ataques aos órgãos que vem sendo observado nos últimos anos (Alves et al., 2022)(Queiroz et al., 2022).

Contudo, além da implantação de *frameworks* de SC, tais como a série ISO 27000; o NIST CSF; o CIS *Controls*; ou o Mitre Att&ck, ou ainda, das próprias iniciativas do Departamento de Segurança da Informação, vinculado ao Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), pouco se discute academicamente sobre os desafios enfrentados pelos gestores na adoção e na implantação dos controles prescritos pelos *frameworks*, e que são muitas das vezes, positivados pelas normas do DSIC.

Para Shapira et al. (2021), alguns pontos acabam por impactar o enfrentamento aos desafios impostos pelo mundo cibernético: a falta de uma arquitetura da informação, a falta de conhecimento sobre as ameaças, procedimentos e tecnologias de segurança cibernética, o desconhecimento dos danos potenciais causados por ataques cibernéticos, uma comunicação incompleta e pouco eficaz aos funcionários, a falta de uma definição

clara da responsabilidade e autoridades, a não familiarização com as regulamentações relevantes, a falta de profissionais dedicados no mercado, aumentando a dependência de serviços externos, e regulamentos imprecisos e incompletos acessíveis ao público.

Nesse sentido, o objetivo geral desse trabalho é mapear os principais desafios da SC na setor público federal brasileiro sob a ótica de gestores de TI, realizando-se entrevistas semiestruturadas com gestores de TI dessse setor, com o objetivo de identificar os desafios. Além dessa introdução, o trabalho apresenta outas quatro seções. Na seção dois fez-se a revisão da literatura. Na seção três descreve-se a metodologia utilizada na pesquisa. A seção quatro dedica-se à análise e discussão, e por fim, a quinta seção dedica-se às conclusões dos autores.

2. Revisão de Literatura

2.1. Gerenciamento de Risco

Para Maček et al. (2021), o principal objetivo do gerenciamento de risco é a redução dos riscos a um nível aceitável, relacionando ao apetite de risco da gestão organizacional, sendo a seleção de soluções adequadas de TI que atendam aos negócios e, também, aos requisitos regulatórios, conformidade e segurança. Entretanto, a escolha de soluções de TI é um processo complexo, caro e que toma tempo, que, muitas vezes, acabam por não alcançar o nível adequado de segurança devido a um aumento de ameaças, tornando-se um desafio a ser enfrentado.

Para Alshahrani et al. (2022), o gerenciamento de risco relacionado à TI é crucial na defesa dos ativos de dados de uma empresa, sendo seu principal objetivo a garantia da proteção da infraestrutura relacionadas à Tecnologia da Informação e Comunicação (TIC). Para os autores, o gerenciamento de risco não deve se limitar aos especialistas de TI, devendo ser uma tarefa crítica no gerenciamento de riscos da empresa.

Kitsios et al. (2022) abordam as etapas previstas pela norma ISO 31000:2018: "(1) definição de escopo, contexto e critérios; (2) avaliação de risco (incluindo identificação de risco, análise de risco e avaliação de risco); (3) tratamento de risco; (4) coleta de dados e relatórios; (5) monitoramento e revisão; e (6) comunicação e consulta". Os autores informam que a norma não tem como papel a imposição de sistemas de gestão de risco uniformes, mas estabelece princípios, uma estrutura e métodos, podendo abranger qualquer tipo de risco, e em todos os setores da economia.

Uma avaliação de riscos de negócios / missão de uma organização é um fator chave para a priorização das mitigações de riscos, se demonstrando um desafio complexo a decisão, poderação e quantificação dos critérios que farão parte desse processo, envolvendo múltiplas partes interessadas. A proteção de ativos valiosos e a minimização de ameaças à segurança da informação requererá uma ampla e abrangente implementação da avaliação de riscos. Sendo feita de forma inadequada, confidencialidade, integridade e disponibilidade poderão estar comprometidas. A avaliação de riscos, que faz parte do gerenciamento de risco, associados à segurança da informação é um processo em que a descoberta, a correção e a prevenção de problemas de segurança devem ser seus principais objetivos (Awang et al., 2020).

2.2. Segurança Cibernética (SC)

A SC é um dos grandes desafios a ser enfrentado pelos governos de diversos países, particularmente no que se refere à garantia do funcionamento de infraestruturas críticas, tais como energia, defesa, transporte, telecomunicações, finanças, entre outros (Moresi et al., 2012). A sua importância tem aumentado à medida que as atividades governamentais e empresariais do dia a dia migram para o ambiente on-line. A digitalização dos processos de trabalhos por parte das organizações será observada a carência de recursos organizacionais, destacando-se os tecnológicos e os humanos, que são chave para o sucesso a longo prazo (Kshetri, 2016), mas, por outro lado, são negligenciadas nas priorizações e, consequentemente, os seus procedimentos preventivos nesta matéria são ainda ligeiramente incipientes (Costa et al., 2019).

A ciber-resiliência passa a ser um ponto a ser alcançado para as infraestruturas críticas, possibilitando, de forma holística, o alinhamento entre a infraestrutura e o negócio da organização, trazendo confiança ao sistema, permitindo a prevenção, absorção, recuperação e adaptação após emergências (Bejarano et al., 2021).

A resiliência cibernética se caracteriza pela proteção efetiva com resposta adequada às ameaças no espaço cibernético, a preservação e a continuidade das atividades e serviços fundamentais, sempre que possível, e a recuperação imediata das operações (Sharkov, 2016).

Diversos governos têm demonstrado preocupação com a temática. A título de exemplo, destaca-se o governo austríaco, que desenvolveu, em 2013, a sua estratégia de SC, descrevendo os desafios, riscos e ameaças com base na análise do ambiente de segurança daquele país. A estratégia leva em consideração sete campos de ação: estruturas e processos, governança, proteção de infraestruturas críticas, legislação, sensibilização e capacitação, gestão de riscos, cooperação internacional (Kaponig, 2020).

O documento se assemelha com a Estratégia de Segurança Cibernética (E-Ciber) do governo brasileiro, entretanto o relatório brasileiro apresenta muito mais ações a serem implementadas, sem contudo, identificar os desafios.

A SC visa à proteção do próprio espaço cibernético, das informações que trafegam por ele, das áreas de TIC que dão suporte a esse ciberespaço, das pessoas que se utilizam dele, assim como de seus interesses (Larsen & Lund, 2021). A maioria dos ataques cibernéticos é evitável, devendo fazer parte uma cultura de segurança cibernética com foco na proteção de sistemas de informações, redes de computadores, dados e usuários que utilizam o ciber espaço (Herath et al., 2022). Para Desolda et al. (2021), a segurança cibernética envolve segurança, salvaguardas, políticas, diretrizes, abordagens de gerenciamento de riscos, boas práticas, ferramentas com foco na proteção do ambiente cibernético e nos ativos de risco.

Na busca por fatores críticos de sucesso relacionados à segurança cibernética, Yeoh et al. (2022) elaboraram uma revisão sistemática da literatura, na qual informam que 68% da liderança empresarial acredita que os riscos relacionados à SC estão aumentando, trazendo como exemplo um ataque de ransomware, em 2021, à área de TI da Colonial Pipeline, provocando o desligamento do maior oleoduto dos Estados Unidos, responsável

por 45% do suprimento de combustível da costa leste norte-americana. Para Yeoh et al. (2022), a busca por medidas que tragam sucesso à SC contempla compreensão dos fatores críticos de sucesso da SC. A formulação das estratégias organizacionais não tem levado em consideração os riscos associados à introdução de novas tecnologias, dentre elas a Internet das Coisas (IoT), mídia social, big data e inteligência artificial (IA).

2.3. A Segurança Cibernética no setor público do Brasil

A E-Ciber define SC como uma arte focada na continuidade da Sociedade da Informação, buscando a a garantia e proteção do espaço cibernético, de seus ativos de informação, assim como de suas infraestruturas críticas (Brasil, 2015). São planos que direcionam o Estado para a melhoria da resiliência, assegurando a segurança de infraestruturas, de serviços e, consequentemente, a segurança do cidadão (Hurel, 2021).

No Brasil, a SC encontra-se sob responsabilidade do DSIC/GSI/PR, responsável pela coordenação do Comitê de Segurança da Informação, além de outros órgãos, como Grupos de Trabalho e Grupos Técnicos relacionados à Segurança das Infraestruturas Críticas, Segurança das Infraestruturas Críticas da Informação, Segurança Cibernética e Criptografia. Ou seja, não existe um órgão específico parar coordenar a SC no país. Assim sendo, a dimensão e a assimetria da estrutura de SC do país representa um desafio a ser enfrentado pelo Brasil (Brasil, 2015).

Evidencia-se, assim, os desafios enfrentados pelo Governo Federal brasileiro, em especial a ausência de um órgão central que exerça coordenação executiva de tais temas, de forma sistêmica e participativa – "multistakeholders" e multissetores, somada a ausência de destaque orçamentário específico e adequado ao tamanho do problema, além da falta de incentivo na criação de órgãos específicos relacionados à SC. Somados à carência do estabelecimento de governança da Segurança da Informação e Comunicações (SIC) e da SC, e da segurança dos ativos de informação críticos (Brasil, 2015).

Segundo o governo brasileiro, são essenciais ações colaborativas entre o Setor de Defesa e a comunidade acadêmica nacional, e os setores público e privado para, assim, contribuir para o desenvolvimento do potencial nacional na área da TI. Além de propor ações no setor, com objetivo de tornar a SC cada vez mais relevante e eficiente, também recomenda que cada órgão do setor público e do setor privado, planeje e realize gestões no sentido de alcançar as propostas do plano, em um esforço conjunto e dedicado, em prol do pleno alcance dos objetivos estratégicos do país, no tema da SC (Decreto Nº 10.222, de 5 de Fevereiro de 2020, 2020).

3. Metodologia

Trata-se de uma pesquisa de natureza aplicada, com objetivos descritivos e exploratórios. Ela é descritiva pois "tem como principal objetivo descrever características de determinada população, fenômeno ou estabelecimento de relações entre variáveis" (Gil, 2002, p. 42). Ela é exploratória pois tem a intenção de se ter maior familiaridade com o problema estudado, compreendendo os desafios que os gestores da administração pública federal enfrentam na gestão da SC. Ainda nesse quesito, Marconi & Lakatos (2022) informam que a pesquisa exploratória permite que a coleta dos dados pode se

dar por meio de entrevistas com pessoas experientes em relação ao assunto, situando-se na abordagem qualitativa, pois buscou-se a compreensão detalhada dos significados por meio de percepções dos entrevistados.

Com isso, elaborou-se um roteiro com 15 perguntas abertas que serviram como roteiro para entrevistas semiestruturadas em profundidade. Selecionaram-se, para essas entrevistas, entrevistados que possuem função de gestor do setor público federal que tenham experiência da área de SC. Dessa forma, o mapeamento dos desafios seria mais claro a partir das respostas dos entrevistados. Foram realizadas 9 entrevistas com indivíduos de organizações públicas federais dos três poderes da república brasileira: executivo, legislativo e judiciário. As entrevistas foram realizadas por meio de videoconferência, entre os meses de março e abril de 2022.

Após a transcrição das entrevistas, utilizou-se a técnica de análise de conteúdo como mais adequada para análise dos dados, que por meio de procedimentos sistemáticos permite inferir conhecimento dos discursos analisados seguindo as etapas propostas em Marconi & Lakatos (2022): (i) pré-análise; (ii) exploração do material; e (iii) tratamento dos resultados, a inferência e a interpretação. A etapa de pré-análise, consistiu na transcrição das entrevistas para organizar as informações e obter um material consistente e pronto para a análise. Assim, realizou-se uma análise prévia das transcrições das entrevistas a fim de destacar trechos importantes que poderiam estar alinhados aos objetivos da pesquisa, ou seja, a partir das respostas dos gestores, mapear os principais desafios relacionados à SC no setor público. A Tabela 1 traz uma visão sucinta do perfil dos entrevistados.

Nr	Poder	Órgão	Função	Experiência em TI
1	*Legislativo*	Senado	Analista em Tecnologia da Informação	19 anos
2	*Executivo*	Ministério das Relações Exteriores	Gerente em Segurança da Informação	5 anos
3	*Judiciário*	Funpresp-Jud	Gerente de Tecnologia da Informação	16 anos
4	*Executivo*	ITI	Coordenador de Tecnologia da Informação	12 anos
5	*Judiciário*	CJF	Subsecretário de Tecnologia da Informação	13 anos
6	*Judiciário*	STJ	Coordenador de Segurança da Informação e Defesa Cibernética	25 anos
7	*Legislativo*	Camara dos Deputados	Coordenação de Administração de Infraestrutura de TIC	23 anos
8	*Judiciário*	STJ	Chefe de Seção – Governança de TIC	35 anos
9	*Executivo*	Ministério do Turismo	Subsecretário de Tecnologia da Informação	13 anos

Tabela 1 – Perfil dos entrevistados

Na segunda etapa, de exploração do material, os trechos destacados foram analisados e agrupados constituindo construtos, ou seja, temas ou frases capazes de representar um grupo de características citadas pelos entrevistados conforme o julgamento do pesquisador e das impressões observadas. Por fim, como etapa final, precedeu-se com o tratamento das informações obtidas através da análise anterior permitindo, assim, a sua interpretação, reflexão e discussão com a literatura.

4. Resultados e Discussão

A Tabela 2 consolida os principais pontos destacados pelos entrevistados, divididos em nove grupos de construtos que representam os desafios da SC no setor público fededral brasileiro. Esses resultados serão apresentados e discutidos com maior detalhe nas seções posteriores.

Construto	Principais apanhados
Infraestrutura de TI	Equipamentos defasados, falta de investimento em softwares adequados, burocracia no processo de aquisição, a necessidade de padronização de processos de trabalho, aumento de relevância das ações de TI, softwares desatualizados, e inadequação da infraestrutura de TI.
Estrutura	Quanto ao GSI: suas portarias não são operacionais, tem pequena abrangência, e, não possui a automia necessária para a coordenação. Carência de padrão de parâmetros de controle e metodologias entre os órgãos. Necessidade de compartilhamento de boas práticas entre os órgãos. Carência, por parte dos gestores, de orientações práticas.
Governança	Áreas estratégicas não percebem a Segurança Cibernética como ponto elementar. A governança é incipiente ou inexistente. O controle de processos de TI não é efetivo. Distanciamento dos gestores da alta administração. Falta de política específica / modelo de governança da segurança cibernética (GSC)
Ataques cibernéticos e credibilidade	Os ataques cibernéticos são comuns, com foco em obter dados. Foco na imagem do órgão. Necessidade de demonstrar a capacidade de proteção. Há protocolos para mitigar os riscos, e os órgãos têm capacidade de promover a defesa de grupos mais avançados.
Cultura	Mundança cultural é importante, podendo ser mais relevante que tecnologias e práticas, assim como a cultura de que TI é secundária. Necessidade na mudança de hábitos, assim como das áreas estratégicas tratarem a segurança cibernética como fundamental.
Capacitação e Sensiblização	Falta de foco na capacitação dos gestores de TI, com poucos investimentos em cursos mais sofisticados. Falta de visibilidade por parte das áreas estratégicas quanto aos investimentos em capacitação de segurança cibernética. Necessidade de engajamento em relação à segurança cibernética por parte dos servidores, sendo o lado humano o mais vulnerável. Escassez em recursos voltados para à área de segurança cibernética.
Legislação	Há uma preocupação por parte do Estado em relação ao tema. O arcabouço normativo brasileiro possui um bom nível de maturidade, mas ainda com grandes lacunas, e, muitas vezes, com temas muito específicos.
E-Ciber	A E-Ciber foi um importante documento para o desenvolimento da Segurança Cibernética no Brasil, ajudando a justificar investimentos na área. As diretrizes não são operacionais, afastando a estratégia da realidade das instituições. Quanto à sua colocação em prática, há gestores que não tiveram conhecimento, e poucos órgãos colocaram suas diretrizes em prática.
Cooperação Internacional	A cooperação internacional é fundamental, com destaque à OCDE. O Brasil possui uma postura independente, e a cooperação não é percebida como uma prática corriqueira.

Tabela 2 – Construtos e Principais apanhados

4.1. Infraestrutura de TI

Para os entrevistados, o setor público possui deficiência na infraestrutura de TI. Alguns gestores afirmaram que os equipamentos e softwares utilizados são defasados, além dos procedimentos não serem adequados para a defesa de constantes ataques, apresentando a existência de equipamentos ultrapassados. Ou seja, investimentos na parte estrutural são necessários para a evolução da SC no país e para tornar a segurança parte elementar em todos os órgãos. Outro ponto destacado foram os processos, já que os gestores majoritariamente afirmaram que falta o foco em prevenção e que, na maioria das vezes, a alta gestão percebe o setor de TI apenas quando existe algum problema, ou quando ocorrem ataques cibernéticos, assim sendo, ações voltadas para a prevenção são, muitas vezes, negligenciadas.

O setor público federal constantemente é alvo de ataques, o que demanda maior cuidado com a segurança. Identificar todos os ataques em tempo real e responder às ameaças de forma efetiva é fundamental (Paiva, 2020). Portanto, a sinalização de falta de infraestrutura de TI adequada torna-se um grande desafio da SC, uma vez que é fundamental existir na organização uma infraestrutura adequada para a manipulação dos dados e do bom funcionamento do órgão (Sousa, 2013).

4.2. Estrutura

A maioria dos gestores afirmaram que a estrutura atual não é adequada e que a criação de um órgão central que coordenasse a SC no país seria essencial. Segundo eles, o GSI emite portarias que não são operacionais, e seu trabalho tem abrangência pequena. Na visão da maioria dos gestores, uma agência específica para fazer essa coordenação seria o mais adequado.

Os relatos dos gestores demonstram, entretanto, certa discordância da ótica deles com a literatura. Segundo Souza & Almeida (2016), o Estado brasileiro possui uma estrutura basilar pronta para atuar nas áreas de segurança e defesa cibernética, ainda que em desenvolvimento, perante os desafios presentes.

4.3. Governança

Para os gestores, existe ainda um grande desafio na GSC da área pública, já que a grande maioria afirma que as áreas mais estratégicas não se importam adequadamente à temática, e a GSC é ainda incipiente. Percebe-se, portanto, a partir das afirmações, a dificuldade de relacionamento entre as áreas mais estratégicas com a parte operacional relacionada à SC, o que aponta para a necessidade de que a temática seja tratada por estruturas vinculadas ao nível estratégico do órgão.

A GSC é ponto fundamental em qualquer instituição, seja pública ou privada. Os processos e a tomada de decisão devem considerar a segurança como aspecto elementar. Os relatos dos entrevistados vão ao encontro do que foi prescrito, por exemplo, na E-Ciber, onde foi descrito que o Brasil ainda precisa fortalecer e aperfeiçoar seus órgãos de governo que tratam das ameaças e que combatem os crimes cibernéticos. Uma vez que o CTIR. Gov é o órgão central do governo que coordena e realiza ações destinadas à gestão de incidentes computacionais, os relatos dos entrevistados sugerem certa reflexão sobre as atribuições desse órgão.

Em complemento, o planejamento e as medidas elaboradas e realizadas não são exemplos de uma governança efetiva com base nas respostas dos entrevistados, pois apresentam lacunas, como superar a falta de comunicação entre a área estrégica e a área de TI. O alinhamento estratégico não tem sido atingido, segundo os gestores, em parte pela falta de percepção da relevância da área de SC para o alcance das metas organizacionais. Importa mencionar sobre a importância da própria estrutura de governança e gestão de riscos para o alcance da eficiência da administração pública brasileira (Nunes et al., 2022).

4.4. Ataques cibernéticos e credibilidade

A preocupação com os constantes ataques cibernéticos se mostrou um dos desafios mais citados perante as vulnerabilidades das instituições. Além dos ataques em si, há preocupação quanto à perda de credibilidade do órgão diante da sociedade.

A tendência é que os ataques cibernéticos a órgãos públicos se tornem cada vez mais sofisticados (Paiva, 2020), e isso tem aumentado a preocupação dos gestores, que destacaram a necessidade de mitigar os ataques com as ferramentas disponíveis, principalmente quando está relacionado a *Advanced Persistent Threats* (APTs). Ao mesmo tempo, verifica-se que ataques já se mostram práticos quanto à própria finalidade de órgãos, por exemplo, quando hackers obtiveram acesso ao sistema processual eletrônico, modificando pareceres, convertendo sentenças de condenação em absolvição e a alterando as contas destinatárias para o recebimento de valores legítimos em processos (Moura & Borges, 2022).

4.5. Cultura

Um desafio apontado pelos gestores é a necessidade de uma mudança cultural nas organizações públicas. Os servidores públicos em geral não enxergam a SC como elementar, apenas como uma área de apoio, o que impede seu desenvolvimento.

Percebe-se, portanto, que há resistência das áreas estratégicas em tratar a SC como tema prioritário nas suas agendas. Isso, é um fator cultural que prejudica o desenvolvimento da SC no país, segundo os gestores. Consequentemente, toda a estruturação da área de TI dentro de um órgão público resta prejudicada com a desconsideração da importância do tema pelas áreas estratégicas.

Para Veiga et al. (2020), os investigadores de SC têm defendido consistentemente que é necessário construir uma cultura de SC para mudar atitudes, percepções, e incutir bons comportamentos de segurança. Isso vai ao encontro com a afirmação dos gestores que alertaram sobre a necessidade da criação de uma cultura de SC para o desenvolvimento do tema no país. Em complemento, onstatou-se necessária uma mudança de ideias, comportamentos e atitudes.

4.6. Capacitação e Sensibilização

Foi perguntado aos gestores se eles acreditavam que os colaboradores de órgãos públicos da área de SC possuem a capacitação adequada e se os órgãos publicos forneciam essa capacitação. Segundo eles, os órgãos fornecem a capacitação adequada,

porém, existe uma resistência para liberar recursos para cursos específicos, uma vez que os superiores não enxergam a importância nesse investimento. Outro ponto que foi destacado é o da sensibilização dos gestores, segundo os entrevistados é difícil gerar interesse e engajamento dos colaboradores em geral, sem a sensibilização da importância da SC.

Assim sendo, a sensibilização dos colaboradores em geral torna-se outro desafio para manter a segurança e mitigar os riscos presentes no dia a dia. Alertar e conscientizar os colaboradores é ponto fundamental, uma vez que o fator humano é o ponto de maior vulnerabilidade dentro da área de segurança da informação, segundo os gestores. A capacitação dos funcionários é essencial segundo afirmação dos gestores nas entrevistas. As organizações não devem apenas fornecer treinamento e recursos para seus funcionários (Chatterjee, 2019), mas também devem criar e manter uma cultura de conscientização de SC (Norris et al., 2019).

4.7. Legislação

A legislação em SC é um ponto de grande discussão: enquanto alguns teóricos afirmam que as leis são essenciais para o desenvolvimento da segurança em um país, outros afirmam que o excesso de burocracia pode atrapalhar. O Brasil possui algumas leis específicas para a temática podendo-se citar: o Marco Civil da Internet; a Lei de Acesso à Informação; e a Lei Geral de Proteção de Dados.

Os entrevistados foram perguntados sobre o nível de maturidade e sobre a importância dessas legislações na área pública. Segundo grande parte dos gestores, o arcabouço normativo brasileiro tem um bom nível de maturidade, porém em certos pontos, faltam diretrizes mais operacionais, já que as legislações atuais são mais estratégicas e muitas vezes não tem efeito prático. Segundo os gestores, as leis não são tão efetivas no nível operacional pois faltam orientações para os problemas que os gestores encontram dentro das organizações diariamente.

4.8. E-Ciber

A E-Ciber foi um marco na legislação brasileira acerca do tema SC. O documento estabeleceu políticas e diretrizes a serem seguidas pelos órgãos da Administração Pública. Assim sendo, os entrevistados foram questionados se o órgão em que eles trabalham absorveram as orientações do documento e se a estratégia se mostrou relevante para a área pública em geral.

Isto posto, a E-Ciber mostrou-se um documento importante para a SC brasileira, porém as diretrizes propostas foram criticadas pelos gestores, devido à falta de orientações práticas na sua implementação o que a afasta da realidade das instituições.

Os relatos indicaram que os normativos brasileiros são de desconhecimento de alguns entrevistados, e um exemplo disso foi a E-Ciber, formalizada por meio de um decreto para área que alguns gestores desconhecima a existência. Isso pode sinalizar certa necessidade de alinhamento entre o que a legislação descreve e a realidade vivenciada pelos gestores.

4.9.Cooperação Internacional

Os gestores foram questionados, de forma geral, como eles enxergavam a importância da cooperação internacinal sobre SC entre os países. Alguns afirmaram que não tinham conhecimento suficiente para opinar, porém alguns afirmaram que essa cooperação é fundamental, no entanto, protegendo a soberania nacional do Brasil, uma vez que existem dados que são extremamente sigilosos e não podem ser compartilhadas. Portanto, os gestores alertam sobre a importância da cooperação entre os países para o desenvolvimento geral, como o compartilhamento de boas práticas. Os relatos obtidos, de certa maneira, alinham-se a literatura. A cooperação internacional sobre a SC embora seja tema complexo e delicado, evidenciou-se, acordo com revisão de literatura, como essencial para o desenvolvimento da SC entre os países.

5. Conclusões

A Segurança Cibernética é fundamental para qualquer organização. São ações e práticas que guiam as organizações com o objetivo de se protegerem contra ataques. Posto isto, nas organizações públicas a SC deve ser vista como fundamental, uma vez que todo o Estado depende do bom funcionamento dos processos tecnológicos e da proteção contra ataques cibernéticos. Observando a dinâmica da SC no setor público no Brasil, este trabalho teve como objetivo mapear os principais desafios da segurança cibernética no setor público federal do Brasil, na ótica de gestores de TI.

Os principais resultados evidenciaram a necessidade de sensibilização dos gestores de níveis mais estratégicos acerca da segurança cibernética em todos os processos da organização. A grande maioria dos gestores afirmam que possuem dificuldades em tornar a segurança como ponto elementar. Outro desafio citado foi a necessidade de mudança cultural dos servidores em geral, pois na ótica dos entrevistados eles não tratam a segurança cibernética como prioridade, consequentemente, tal desconsideração pode se tornar um ponto de vulnerabilidade.

Um outro importante desafio que foi identificado foi a carência de diretrizes operacionais para que os gestores executem suas tarefas. Os entrevistados informaram que a legislação brasileira possui um bom nível de maturidade no campo estratégico, porém, faltam orientações funcionais que os instrua nas suas rotinas.

Ademais, estes resultados refletem a análise das entrevistas realizadas com 9 gestores do setor público que trabalham diretamente com a SC, portanto, o estudo realizado apresentou limitações quanto ao número de entrevistados, uma vez que por ser um tema delicado, alguns gestores recusaram a participação o que permitiu considerar os resultados encontrados considerando os relatos dos entrevistados da Tabela 1. Outro ponto a ser lembrado é que as entrevistas são uma representação do discurso pessoal em um período específico e não necessariamente refletem o discurso dos gestores em outros períodos.

Acredita-se que este trabalho possa contribuir para uma discussão cada vez mais aprofundada sobre a SC no setor público no Brasil. Compreender os desafios é elementar para encontrar pontos de superação e desenvolver a SC no país. Como citado anteriormente, as pesquisas referentes ao tema no país ainda iniciais e como estudos

futuros novas pesquisas podem ser executadas em outros períodos e com um número maior de participantes. Dessa forma, sugere-se como trabalhos futuros a própria continuidade e alargamento do estudo; a validação dos construtos identificados por meio de propriedades psicométricas; e o uso desses construtos para formar a base de um questionário consolidado a ser aplicado às instituições do governo federal brasileiro como forma de identificar a evolução e o desenvolvimento da SC no país ao longo dos próximos anos. Além disso, as questões também poderão subsidiar pesquisas de natureza similar em organizações públicas de outros países.

Agradecimentos

O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas; da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022; e do Departamento de Administração da Universidade de Brasília, por meio dos recursos provenientes da Resolução ADM/UnB 01/2016.

Referências

Alshahrani, H. M., Alotaibi, S. S., Ansari, M. T. J., Asiri, M. M., Agrawal, A., Khan, R. A., Mohsen, H., & Hilal, A. M. (2022). Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Applied Sciences 2022, Vol. 12, Page 5911*, *12*(12), 5911. https://doi.org/10.3390/APP12125911

Alves, R. S., Georg, M. A. C., Nunes, R. R. (2022). Judiciário sob ataque hacker: fatores de risco para a segurança do processo decisório em sistemas judiciais eletrônicos. *Encontro de Administração da Justiça - ENAJUS*.

Awang, N., Samya, G. N., Hassana, N. H., Maaropa, N., Magalingama, P., & Kamaruddina, N. (2020). Identification of Information Security Threats Using Data Mining Approach in Campus Network. *Journal of Physics: Conference Series*, *1551*(1), 12. https://doi.org/10.1088/1742-6596/1551/1/012006

Bejarano, M. H., Rodriguez, R. J., & Merseguer, J. (2021). A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks. *Iberian Conference on Information Systems and Technologies, CISTI*. https://doi.org/10.23919/CISTI52073.2021.9476324

Brasil. (2015). Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018. In *DOU*.

Brasil. (2018). Decreto nº 9.637, de 26 de dezembro de 2018, (2018). https://www.in.gov.br/materia/-/asset_publisher/KujrwoTZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938

Decreto nº 10.222, de 5 de fevereiro de 2020, (2020). https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419

Chatterjee, D. (2019). Should executives go to jail over cybersecurity breaches? *Https://Doi.Org/10.1080/10919392.2019.1568713*, *29*(1), 1–3. https://doi.org/10.1080/10919392.2019.1568713

Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). The Security Challenges Emerging from the Technological Developments: A Practical Case Study of Organizational Awareness to the Security Risks. *Mobile Networks and Applications*, *24*(6), 2032–2037. https://doi.org/10.1007/S11036-018-01208-0/FIGURES/8

Desolda, G., di Bari Aldo Moro LAUREN FERRO, U. S., Marrella, A., Catarci, T., Francesca Costabile, M., & di Bari Aldo Moro, U. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Comput. Surv*, *54*. https://doi.org/10.1145/3469886

Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Https://Doi.Org/10.1080/23738871.2020.1728355*, *5*(1), 9–29. https://doi.org/10.1080/23738871.2020.1728355

Gil, A. C. (2002). *Como classificar as pesquisas. Como elaborar projetos de pesquisa*.

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy 2022, Vol. 2, Pages 1-18*, *2*(1), 1–18. https://doi.org/10.3390/JCP2010001

Hurel, L. M. (2021). *Uma análise da estratégia nacional de cibersegurança - Instituto Igarapé*. https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/

Kaponig, M. G. H. (2020). Austria's national cyber security and defense policy: Challenges and the way forward. *Connections*, *19*(1), 21–37. https://doi.org/10.11610/CONNECTIONS.19.1.03

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, *14*(3), 1269. https://doi.org/10.3390/su14031269

Kshetri, N. (2016). Cybersecurity and Development. *Markets, Globalization & Development Review*, *1*(2). https://doi.org/10.23860/MGDR-2016-01-02-03

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Maček, D., Magdaleni´c, I. M., Begičevi´, N., Re, B., Francisco, A., & López De Hierro, R. (2021). A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment. *Mathematics 2021, Vol. 9, Page 1045*, *9*(9), 1045. https://doi.org/10.3390/MATH9091045

Marconi, M. de A., & Lakatos, E. M. (2022). *Metodologia Científica. Edição do Kindle* (Editora At).

Moresi, E. A. D., Santini Júnior, N., Fragola, R. J., Bassi, M. C., & Alonso, J. E. T. (2012). Defesa cibernética: um estudo sobre a proteção da infra-estrutura e o software seguro. *Conferencia Iberoamericana de Complejidad, Informática Y Cibernética*. https://bit.ly/3bSjRQi

Moura, R. M., & Borges, L. (2022, March 28). *A impunidade dos hackers que colocaram o Judiciário de joelhos*. Veja. https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, *79*(6), 895–904. https://doi.org/10.1111/PUAR.13028

Nunes, R. R., Perini, M. T. B. S., Pinto, I. E. M. M. (2021). A gestão de riscos como instrumento para a aplicação efetiva do Princípio Constitucional da Eficiência. *Revista Brasileira de Políticas Públicas*, 11(3), 259-281. https://doi.org/10.5102/rbpp.v11i3.7903

Paiva, Y. C. (2020, October 20). *Conscientização sobre segurança cibernética na Administração Pública*. Conteúdo Jurídico. https://conteudojuridico.com.br/consulta/artigos/55351/conscientizao-sobre-segurana-ciberntica-na-administrao-pblica

Queiroz, C. E. M., Nunes, R. R., Cunha, J. H. C, Silveira Junior, A. (2022). Os Tribunais do Distrito Federal possuem estruturas para gerenciar riscos de segurança da informação? Um estudo à luz das três linhas de defesa. *Encontro de Administração da Justiça - ENAJUS*.

Shapira, N., Ayalon, O., Ostfeld, A., Farber, Y., & Housh, M. (2021). Cybersecurity in Water Sector: Stakeholders Perspective. *Journal of Water Resources Planning and Management*. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001400

Sharkov, G. (2016). From Cybersecurity to Collaborative Resiliency. *ACM Digital Library*. https://doi.org/10.1145/2994475.2994484

Sousa, E. S. de. (2013). A gestão da TI dentro do serviço público. *Gestão e Tecnologia Para Competitividade*. https://www.aedb.br/seget/arquivos/artigos13/25218236.pdf

Souza, E. A. A. de, & Almeida, N. N. de. (2016). A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do estado. *Revista Da Escola de Guerra Naval*, *22*(2), 381–410. https://doi.org/10.21544/1809-3191/REGN.V22N2P381-410

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1–22. https://doi.org/10.14763/2020.4.1533

Veiga, A. da, Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/J.COSE.2020.101713

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers and Security*, *118*. https://doi.org/10.1016/j.cose.2022.102724