Universidade de Brasília
Faculdade de Administração, Contabilidade, Economia e Gestão de Políticas Públicas
Departamento de Administração

WALISSON MAGNO SILVA RODRIGUES

CONDICIONANTES DA SEGURANÇA CIBERNÉTICA NA ÁREA PÚBLICA FEDERAL DO BRASIL SOB A ÓTICA DOS GESTORES: desafios, benefícios e oportunidades

Brasília – DF
2022

WALISSON MAGNO SILVA RODRIGUES

CONDICIONANTES DA SEGURANÇA CIBERNÉTICA NA ÁREA PÚBLICA FEDERAL DO BRASIL SOB A ÓTICA DOS GESTORES: desafios, benefícios e oportunidades

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador:

Dr. Rafael Rabelo Nunes

Brasília – DF

2022

WALISSON MAGNO SILVA RODRIGUES

CONDICIONANTES DA SEGURANÇA CIBERNÉTICA NA ÁREA PÚBLICA FEDERAL DO BRASIL SOB A ÓTICA DOS GESTORES: desafios, benefícios e oportunidades

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do aluno

Prof. Dr. Rafael Rabelo Nunes
Professor-Orientador

Dr. Rildo Ribeiro dos Santos
Examinador

Dr. Carlos André de Melo Alves
Examinador

AGRADECIMENTOS

Agradeço a Deus, que sempre me sustentou e me protegeu. Agradeço aos meus pais que abriram mão de suas vidas para criarem seus cinco filhos. Com muito trabalho e doação da própria vida nos mostraram que a educação era tudo que podiam nos dar. Aos meus irmãos, que sempre estenderam suas mãos e nunca me negaram nada. Agradeço ao meu orientador Dr. Rafael Rabelo Nunes, por ter acreditado no meu potencial, pelo apoio e empenho dedicado a este trabalho, além de todos os ensinamentos que contribuíram no meu processo de formação profissional. Agradeço a todos os professores que tive durante toda minha vida escolar e acadêmica, cada um deles contribuiu no meu processo de formação profissional.

RESUMO

A Segurança Cibernética vem ganhando papel de destaque em diversas frentes da sociedade e se mostra imprescindível em todos os setores. Na área pública brasileira não é diferente, o governo define, por meio de suas diretrizes, como sendo um tema fundamental em todas as frentes da área pública. Nesse sentido, o objetivo do trabalho foi mapear os principais condicionantes da gestão segurança cibernética na área pública do Brasil sob a ótica dos gestores. Assim sendo, foram realizadas entrevistas semiestruturadas com gestores da área pública federal, que trabalham na área de segurança cibernética, para identificar e mapear os principais condicionantes encontrados. As entrevistas, posteriormente, foram analisadas por meio de análise de conteúdo para formar construtos que representassem os principais condicionantes encontrados pelos entrevistados. A partir do resultado, identificaram-se 9 construtos que representam os condicionantes do campo de segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI .

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

ABSTRACT

Cybersecurity has been gaining a prominent role in several fronts of society and is essential in all sectors. In the Brazilian public area it is no different, the government defines, through its guidelines, as a fundamental and very important theme in all fronts of the public area. In this sense, the objective of this work was to map the main conditioning factors of the management of cybersecurity in the public area in Brazil from the perspective of the managers. Therefore, semi-structured interviews were conducted with managers of the federal public area, who work in the area of cybersecurity, to identify and map the main constraints found. The interviews were subsequently analyzed by means of content analysis to form constructs that represented the main conditioning factors found by the interviewees. As from the result, it was identified 9 constructs that represent the conditioning factors of the cybersecurity field in the Brazilian federal public administration from the perspective of IT managers.

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

LISTA DE ILUSTRAÇÕES FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
ANPD - Autoridade Nacional de Proteção de Dados
APF - Administração Pública Federal
BRICS - Building Better Global Economic BRICs
CERT - Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
CSIRT - Computer Security Incident Response Team
DOU - Diário Oficial da União
DSI - Departamento de Segurança da Informação
E-CIBER - Estratégia Nacional de Segurança Cibernética
END - Estratégia Nacional de Defesa
FEM - Fórum Econômico Mundial
GSC - Governança da Segurança Cibernética
GSIPR - Gabinete de Segurança Institucional da Presidência da República
IPEA - Instituto de Pesquisa Econômica Aplicada
ISO - International Organization for Standardization
LGDP - Lei Geral de Proteção de Dados
NIST - National Institute of Standards and Technology
NSA - National Security Agency
OCDE - Organização para a Cooperação e Desenvolvimento Econômico
OMS - Organização Mundial da Saúde
PNSIC - Política Nacional de Segurança de Infraestruturas Críticas
SEGCIBER - Segurança Cibernética
SERPRO - Serviço Federal de Processamento de Dados
SIC - Segurança de Infraestruturas Críticas
STJ - Superior Tribunal de Justiça
SUS - Sistema Único de Saúde
TCU - Tribunal de Contas da União
TI - Tecnologia da Informação
TIC - Tecnologias da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

O rápido desenvolvimento da internet e o avanço tecnológico em todos os setores da sociedade fizeram com que ameaças cibernéticas se tornassem um tema de grande preocupação. Vulnerabilidades são exploradas por atacantes diariamente em um conflito de interesses. A segurança cibernética, então, tornou-se um tema complexo, sendo seu conhecimento essencial para qualquer pessoa ou organização, já que abrange uma vasta 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).

Um estudo divulgado pelo site Statista revela que, no primeiro semestre de 2020, 4,66 bilhões de usuários estavam ativos na rede, o que representa, em média, 59% da população mundial (JOHNSON, 2021). Por conseguinte, um estudo da consultoria Canalys apontou que 2020 registrou mais dados comprometidos por ataques do que os 15 anos anteriores combinados, foram mais de 30 bilhões de dados acessados ilegalmente por invasores. Ao mesmo tempo, os gastos com protocolos de cibersegurança também registraram um aumento de 10% em relação a 2019, atingindo US$ 53 bilhões globalmente (BALL, 2020).

Na área pública brasileira, os ataques cibernéticos a órgãos públicos tornaram-se frequentes, isto pode ser exemplificado com o ataque ao STJ no ano de 2020, o ataque cibernético criptografou dados e forçou o tribunal a suspender sessões e tirar seu site do ar, afetando os sistemas do órgão por semanas (PONTES, 2020). Outro ataque relevante afetou os sistemas e os sites do Ministério da Saúde e do ConecteSUS no ano de 2021 (CASTRO, 2021). O que tornou necessária uma atenção redobrada no que se refere à segurança da informação, pois derrubar um site público ou roubar informações sigilosas traz notoriedade ao *hacker* perante outros criminosos. Além disso, ele pode utilizar esses dados para fazer chantagem, exigindo dinheiro para o resgate (PAIVA, 2020).

A rápida evolução tecnológica aliada a uma maior complexidade dos sistemas, exige um maior nível de preocupação com a segurança da informação organizacional. Em um ambiente de negócios, as organizações são altamente dependentes do uso da Internet, como resultado do

desenvolvimento tecnológico. Portanto, 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).

Essa rápida mudança no ambiente organizacional, trouxe desafios complexos relacionados à segurança cibernética, as rápidas transformações na economia e na sociedade, proporcionadas pelo ambiente digital, impuseram novas ações e estratégias na área pública brasileira (BRASIL, 2018). Assim sendo, considerando tal contexto de transformação, este estudo busca identificar e mapear os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI.

1.1 Formulação do problema

A partir dos dados supracitados pode-se observar a relevância do tema Segurança cibernética, o tema vem ganhando papel de destaque em diversas frentes da sociedade e se mostra imprescindível a todos os setores. O governo brasileiro afirma que a segurança cibernética se trata de um tema transversal, multidisciplinar e multissetorial (BRASIL, 2020). Entretanto, percebe-se escassez de estudos que aborde os condicionantes específicos dessa temática no setor público brasileiro. Nesse sentido, torna-se relevante o mapeamento desses condicionantes para, assim, após a identificação seja possível encontrar pontos de superação e desenvolvimento. Portanto, a pergunta do problema de pesquisa pode ser definida como:

"Quais são os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI?"

1.2 Objetivo Geral

O objetivo geral desta pesquisa é mapear os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI.

1.3 Objetivos Específicos

a) Identificar e classificar em construtos, os principais condicionantes para a gestão da segurança cibernética de órgãos da administração pública federal;

b) Elaborar roteiro de entrevista semiestruturada com base no conteúdo abordado para conduzir entrevistas visando a

c) Identificar e avaliar os posicionamentos dos entrevistados com relação à segurança cibernética na área pública brasileira;

d) Entrevistar especialistas com experiência em Tecnologia da Informação, segurança, infraestrutura e áreas relacionadas de instituições do Governo Federal;

e) Identificar as maiores tendências da gestão de segurança cibernética e práticas relacionadas no Governo Federal, além de mapear as melhores práticas internacionais para, assim, apresentar pontos de superação para os desafios encontrados.

2 REFERENCIAL TEÓRICO

2.1 Segurança Cibernética

O tema segurança cibernética revelou-se elementar para as pessoas, organizações e Estados desde o começo do século XXI. A segurança cibernética constitui um dos principais desafios para os Estados em matéria de Segurança (CORREIA; SANTOS; BILHIM, 2017). Moresi *et al*. (2012) alertam que a segurança cibernética 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. Apesar disso, a cibersegurança não é normalmente uma das principais prioridades das organizações e, consequentemente, os seus procedimentos preventivos nesta matéria são ainda ligeiramente incipientes (COSTA *et al*., 2019).

O conceito de Segurança Cibernética é abrangente e envolve diversos atores e processos, assim sendo, muitas vezes é confundido com defesa cibernética. A segurança cibernética seja a proteção que se realiza no ciberespaço contra as ameaças a valores ou direitos da comunidade política, assim perpetrados neste novo ambiente digital (GOUVEIA, 2021). Assim sendo, a segurança cibernética compreende aspectos e atitudes, tanto de prevenção quanto de repressão, enquanto a defesa cibernética abrange ações operacionais de combates ofensivos (MANDARINO JÚNIOR; CANONGIA, 2010). Dessa forma, a defesa cibernética está ligada à noção de guerra, enquanto a segurança cibernética está associada à ideia de ilícitos. Definida essa diferença, a União Europeia define o conceito de segurança cibernética como o conjunto de "salvaguardas e ações que se podem empregar para proteger o domínio cibernético, tanto no âmbito civil quanto militar, frente às ameaças vinculadas com suas redes interdependentes e sua infraestrutura de informação, ou que possam afetá-las" (EUROPEAN COMISSION, 2013).

Para o governo brasileiro "segurança cibernética é entendida 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). A sua importância tem aumentado à medida que as atividades governamentais, empresariais e do dia-a-dia em todo o mundo migram para o ambiente on-line.

Mas especialmente nas economias emergentes, "em qualquer organização que digitalize suas atividades carece de recursos organizacionais, tecnológicos e humanos, e outros ingredientes fundamentais necessários para garantir o seu sistema, que é a chave para o sucesso a longo prazo" (KSHETRI, 2016, p. 3). Ou seja, nos últimos anos o tema segurança cibernética vem crescendo exponencialmente em todo mundo, principalmente pelos números de usuários na internet, e consequentemente pelos diversos ataques cibernéticos que acontecem diariamente.

2.2 Ameaças Cibernéticas

Assim como o conceito e as estruturas da segurança cibernética se desenvolveram ao longo dos anos, as ameaças ao mundo cibernético também. Os eventos cibernéticos podem ser maliciosos (cavalos de tróia, *worms* de computador, ataques de sabotagem) ou não intencionais (atualizações incorretas de *software*, protocolos errôneos ou conexões de rede indesejadas), e podem ocorrer no espaço cibernético, no mundo físico, ou em ambos. Sendo assim, o combate a ataques cibernéticos tornou-se uma questão relevante para as empresas, indústrias e governos, especialmente aqueles que dependem fortemente das tecnologias da informação (HUANG *et al*., 2018).

O número de ataques e a sua sofisticação aumentam diariamente, por conseguinte as organizações têm buscado aprimorar seus procedimentos, processos, protocolos e estratégias, com o objetivo de evitar que tais ataques se transformem em incidentes cibernéticos. O Grupo *CyberEdge* estimou que os prejuízos causados por incidentes cibernéticos em 2021 chegaram próximos dos 6 trilhões de dólares, o dobro dos números de 2015. Estes impactos são sentidos não só pelas empresas, mas também por toda a economia (CYBER EDGE GROUP, 2021). Alguns casos recentes exemplificam a relevância dos ataques:

- Um artigo - do jornal diário francês Le Monde sobre o vírus Petya, que recentemente atingiu várias organizações, reportaram perdas econômicas totais para estas empresas devido ao ataque em mais de um bilhão de euros (UNTERSINGER, 2017).
- Em 2020, a Solar Winds, empresa de infraestrutura de informação, sofreu o que pode ser considerado, segundo o presidente da Microsoft, Brad Smith, o “maior e mais sofisticado ataque que o mundo já viu”. Isso porque foram empregadas diversas táticas

e técnicas de invasão e espionagem cibernética. Os hackers inseriram um código malicioso dentro da atualização de software de monitoramento da Solar Winds que foi enviada para até 18 mil clientes. Dentre eles estão as empresas Microsoft e os departamentos de energia, justiça e segurança nuclear dos Estados Unidos (RIGUES, 2021).

- No Brasil um dos ataques mais preocupantes em 2020 foi o ataque direcionado ao Supremo Tribunal de Justiça (STJ). O ataque foi do tipo *ransomware*, no qual os criminosos sequestram dados e exigem pagamento para liberá-los. O ataque afetou cerca de 12 mil julgamentos e ainda gera preocupação referente a dados sigilosos que ficaram à disposição dos criminosos. A investigação sobre o caso está sendo feita pela Polícia Federal em caráter sigiloso. O sistema do STJ ficou uma semana fora do ar e só foi completamente restabelecido após meses (PONTES, 2020).

Os ataques cibernéticos também visaram infraestruturas críticas nacionais, como os serviços de saúde (BURGUESS, 2020). E, com a pandemia do COVID-19 não foi diferente, os números de ataques a serviços da área da saúde aumentaram significativamente, o Fórum Econômico Mundial (FEM) informou que a pandemia levou a um aumento de 50,1% nos ciberataques entre 31 de dezembro de 2019 e 14 de abril de 2020 (FÓRUM ECONÔMICO MUNDIAL, 2020). Os cibercriminosos têm aproveitado a oportunidade decorrente da pandemia para expandir seus ataques (GHANN; TETTEH; DOE, 2022) e atingir infraestruturas críticas da área da saúde. Segundo a *Check Point Research* (CPR), fornecedora líder de soluções de cibersegurança global:

> Os ataques contra hospitais e organizações relacionadas à saúde são particularmente muito prejudiciais porque qualquer interrupção em seus sistemas pode afetar sua capacidade de prestar cuidados e colocar vidas em risco, tudo isso agravado com as pressões que esses sistemas estão enfrentando tentando lidar com o aumento global de casos da COVID-19. É por isso que os cibercriminosos visam especificamente o setor de saúde, pois acreditam que os hospitais têm mais chances de atenderem às suas demandas de resgate (CHECK POINT RESEARCH, 2021)

Alguns casos de ataques a hospitais e sistemas de saúde durante a pandemia da COVID-19:

- Um hospital na República Tcheca foi obrigado a suspender ações contra o coronavírus e remanejar seus pacientes para uma estrutura alternativa após sofrer um ciberataque de natureza não divulgada pelo governo (KHALILI, 2020).

- Hackers de elite tentaram invadir sistemas da Organização Mundial da Saúde (OMS) em 2020, a tentativa de invasão não obteve sucesso. A organização alertou que as ações de hackers contra a agência e seus foram disparadas em meio à campanha do órgão global para combate ao coronavírus (BING, 2020).
- O Hospital Sírio-Libanês, em São Paulo, foi alvo de um ataque. A ação hacker, que tirou do ar o site e o aplicativo do hospital, ocorreu nas primeiras horas do dia 06/07/2020. De acordo com o Hospital, não houve qualquer perda de informação (LOUREIRO, 2020)
- O Ministério da Saúde brasileiro foi alvo de um ataque cibernético que derrubou o seu site na madrugada do dia 10/12/2022. Plataformas importantes no combate à pandemia e de apoio a programas sociais como ConecteSUS, Painel Coronavírus e DataSUS também foram afetadas (CASTRO, 2021).

2.3 Vulnerabilidades

De acordo com a ISO 27000, a norma de Sistemas de Gestão de Segurança da Informação, as vulnerabilidades são “fraquezas de um ativo que poderia ser potencialmente explorado por uma ou mais ameaças”. Essas deficiências podem ocorrer durante o projeto, implementação, configuração ou operação de ativos ou controles. Eles podem ser produzidos na empresa por meio de erro humano, tecnologia desatualizada ou intenção maliciosa. Assim sendo, a vulnerabilidade se refere tanto à fragilidade do software como a do hardware, fraquezas encontradas em processos, políticas e no componente humano de uma organização (HUANG *et al*., 2018)

A informação é crucial para Administração Pública Federal (APF), mas também está exposta a grandes riscos. Os pilares da segurança da informação que são disponibilidade, integridade, confidencialidade e autenticidade, estão sujeitos a vulnerabilidades (MANDARINO JUNIOR; CANONGIA, 2010). A E-Ciber além de apresentar a estratégia nacional e as diretrizes da segurança cibernética no Brasil, também evidenciou vulnerabilidades e pontos que possam ser aprimorados no ambiente cibernético brasileiro. Assim sendo, alguns dos campos importantes acerca das vulnerabilidades são:

a. Falhas humanas: Em uma estrutura de segurança cibernética, o elo mais vulnerável é o fator humano. Ele pode ser responsável por expor dados, interromper sistemas e apresentar portas paras futuras ameaças. De acordo com o governo brasileiro é essencial à sociedade compreender as ameaças e os riscos no espaço cibernético para, assim, possibilitar às pessoas o uso adequado e oportuno de procedimentos e de ferramentas. Alerta-se também, a necessidade de capacitação continuada para profissionais do setor público (BRASIL, 2020).

b. Vulnerabilidades de aplicações: De acordo com a Kaspersky, os cibercriminosos exploram vulnerabilidades não corrigidas em sistemas operacionais e aplicativos comuns, como Java, Adobe, Internet Explorer, Microsoft Office e outros, como parte de ataques direcionados contra organizações de todos os tamanhos (RODRIGUES, 2021). No governo brasileiro, não é diferente, ele definiu na E-Ciber a necessidade de "aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética" (BRASIL, 2020).

c. Vulnerabilidade de Processo: Uma grande porta para as ameaças cibernéticas são falhas em protocolos e processos. Sendo assim, o governo brasileiro identificou a necessidade de elevar o nível de proteção do Governo "recomenda-se estabelecer protocolos e requisitos referentes à prevenção, ao monitoramento, ao tratamento, e à resposta aos incidentes computacionais, voltados principalmente às equipes especializadas que tratam das ameaças cibernéticas." (BRASIL, 2020).

2.4 A segurança cibernética no Brasil

Assim como na maioria dos países emergentes, o Brasil ainda está se estruturando diante aos diversos desafios que surgiram com a emergência do tema segurança cibernética. Pode-se elencar o crescimento do número de usuários na Internet brasileira, consequentemente aumenta-se o número de ataques. Segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil foram reportadas, no ano de 2020, 665.079 notificações de ataques cibernéticos no Brasil (CERT, 2020).

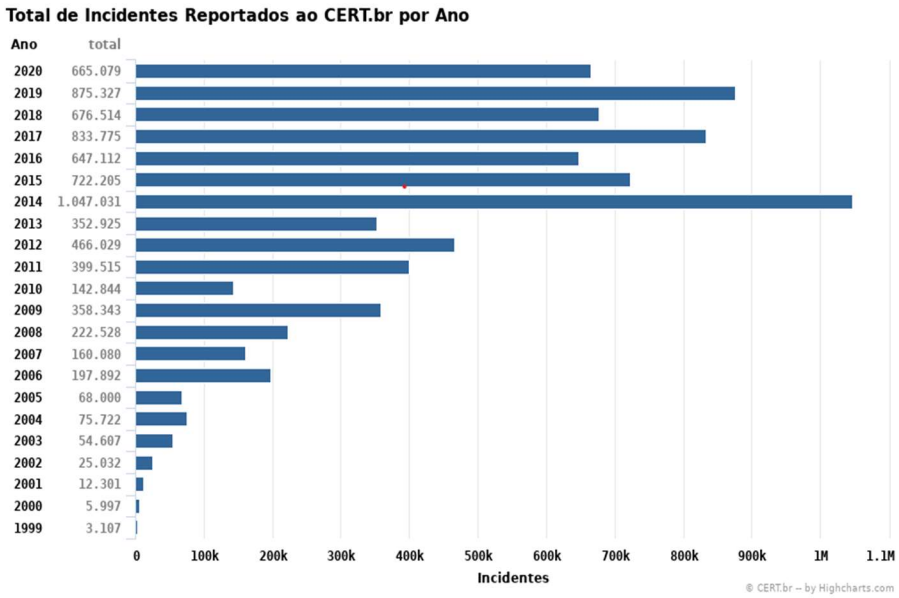

Figura 1: Incidentes reportados no Brasil no ano de 2020

Fonte: CERT.br

Na figura 1, pode-se perceber um aumento de 88% em relação ao ano de 2013. O governo brasileiro alerta sobre a importância das organizações consideraram a segurança cibernética como ação prioritária de investimentos.

> Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralização dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas. Dessa forma, é importante que as organizações, públicas ou privadas, estabeleçam políticas e procedimentos de segurança cibernética que sejam periodicamente revisados, atendam à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores, por meio de programas de capacitação e de treinamento (BRASIL, 2020).

Assim sendo, é essencial o esforço conjunto, entre o governo e as organizações, para tornar a segurança cibernética como parte prioritária nas organizações para, assim, se estruturarem e aprimorarem seus procedimentos de segurança e a capacitarem os colaboradores, com o objetivo de melhoria contínua e eficiente.

2.4.1 A estrutura no setor público

Como citado anteriormente, no Brasil, a segurança e defesa cibernética são apresentadas como conceitos divergentes. Da Cruz Júnior (2013) afirma que:

> A sistematização de instituições e a distribuição de competências entre os organismos para o desenvolvimento de segurança e defesa cibernética é bem recente no Brasil. Algumas instituições que existem há décadas ainda precisam ser adaptadas à nova temática e realidade social. Segurança e defesa cibernética são tratadas no Brasil por diversos organismos. Incluem-se instituições públicas, desde o nível estratégico, de governo, até os operacionais, além da atuação de entidades não governamentais representando o setor privado (DA CRUZ JUNIOR, 2013, p.21).

Ou seja, podemos elencar que a segurança e defesa cibernética no Brasil está estruturada da seguinte forma, as ações relativas à defesa cibernética estão sob a responsabilidade do Comando de Defesa Cibernética, subordinado ao Ministério da Defesa, enquanto aspectos vinculados à segurança cibernética governamental estão na estrutura do Gabinete de Segurança Institucional (GSI), órgão do poder executivo, além disso a existência de diversos entes privados responsáveis pela segurança cibernética, por intermédio de departamentos de segurança da informação ou de informática, esses órgãos apresentam sinergia com os organismos de defesa e segurança cibernética brasileira (GONZALES; PORTELA 2018).

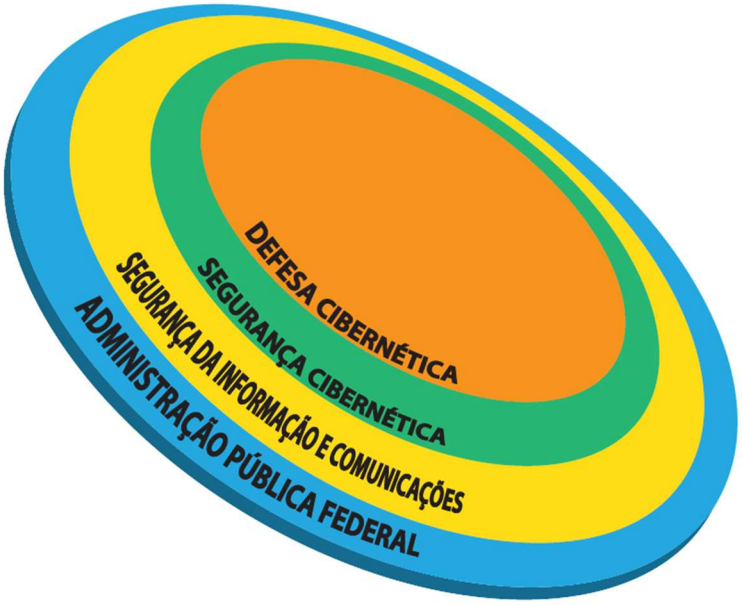

Figura 2: Visão em camadas: SIC e a SegCiber.

Fonte: Estratégia de SIC e a SegCiber, da APF (2015-2018).

Podem-se destacar diversos outros órgãos da Administração Pública Federal que compõe tal estrutura, a exemplo da Polícia Federal (PF), Ministério da Justiça (MJ), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br), Serviço Federal de

Processamento de Dados (Serpro), centros de pesquisa e universitários, além dos profissionais de TI nos órgãos públicos (DA CRUZ JÚNIOR, 2013).

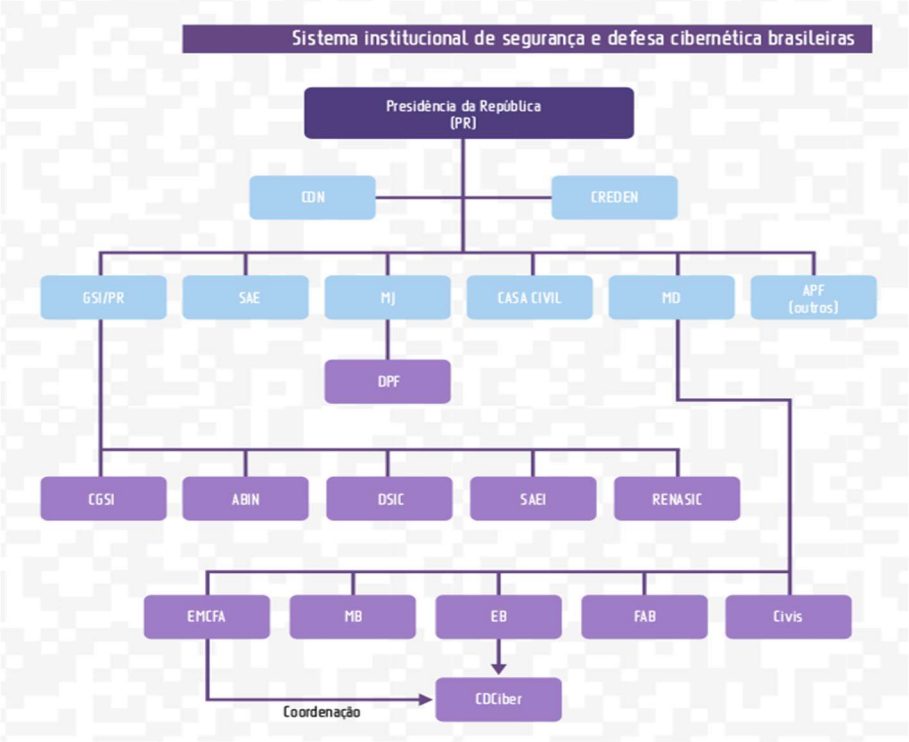

Figura 3: Visão da estrutura da SegCib no Brasil.

Fonte: Brasil (2015) (2011, p. 211 apud IPEA, 2013, p. 22)

2.4.2 A Estratégia Nacional de Defesa

O Ministério da Defesa apresentou, em 2008, a Estratégia Nacional de Defesa (END), com o objetivo de elaborar um plano de defesa focado em ações estratégicas de médio e longo prazo para modernizar a estrutura nacional de defesa. A END, aprovada pelo Decreto no 6.703, de 18 de dezembro de 2008, definiu três setores estratégicos para defesa nacional: nuclear, cibernético e espacial. Delegou à Marinha do Brasil a gerência do programa nuclear; à Força Aérea, o programa espacial; e ao Exército Brasileiro, a liderança da defesa cibernética em território nacional.

> No Setor Cibernético, as capacitações destinar-se-ão ao mais amplo espectro de emprego dual. Incluirão, como parte prioritária, as tecnologias de comunicações entre as unidades das Forças Armadas, de modo a assegurar sua interoperabilidade e a capacidade de atuar de forma integrada, com segurança. Essa condição implica aprimorar a Segurança da Informação e das Comunicações e a Segurança Cibernética,

> em todas as instâncias do Estado, com ênfase na proteção das Estruturas Críticas. Será necessário, portanto, concluir a estrutura do Sistema Militar de Defesa Cibernética com seu marco legal, suas normas afins, bem como desenvolver o seu preparo e o emprego, em todos os níveis. (BRASIL, 2016, p. 55)

O documento afirma que é essencial fomentar a pesquisa, o desenvolvimento e a inovação, com foco nas tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Setor de Defesa e que contribuam com a segurança cibernética no âmbito nacional, envolvendo a comunidade acadêmica doméstica e internacional. Afirma também, que 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 Tecnologia da Informação (BRASIL, 2016).

2.4.3 Estratégia Nacional de Segurança Cibernética

No ano de 2020 o governo brasileiro aprovou sua primeira Estratégia de Segurança Cibernética (E-Ciber). O documento estabeleceu as principais ações do governo (nacional e internacionalmente) na área de segurança cibernética entre os anos 2020-2023. A E-Ciber, buscou preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabeleceu ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. A medida é uma orientação do governo sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética.

> Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Em terceiro, vê-se a existência de diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema (BRASIL, 2020).

O documento apresentou o contexto da segurança cibernética no Brasil, e propõe ações na área com objetivo de tornar o tema 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 crítico e atual tema da segurança cibernética brasileira (BRASIL, 2020). A produção de documentos legais brasileiros os quais fomentam o debate público sobre temas como a segurança cibernética demonstram, cada vez mais, "a percepção pelo Estado brasileiro da potencialidade e dos riscos de ataques cibernéticos às infraestruturas críticas e da segurança da informação no país" (SOUZA e ALMEIDA, 2016, p.10).

2.5 Os condicionantes da segurança cibernética

Após serem apresentados o contexto, conceitos e vulnerabilidades sobre a segurança cibernética, chega-se ao escopo principal da revisão de literatura, os principais condicionantes da segurança cibernética. Busca-se identificar, portanto, por meio da revisão bibliográfica, os principais condicionantes da segurança cibernética no Brasil.

Em Portugal, o Quadro Nacional de Referência para a Cibersegurança apresenta "diversas medidas técnicas e processuais, bem como evidências de implementação que permitam às organizações melhorar a sua capacidade de proteção e de resposta aos desafios do ciberespaço e da segurança da informação" (CENTRO NACIONAL DE CIBERSEGURANÇA, 2019).

Em 2013, o governo austríaco desenvolveu a Estratégia Austríaca de Segurança Cibernética, o documento descreveu os novos desafios, riscos e ameaças, incluindo as ameaças cibernéticas, com base na análise do ambiente de segurança austríaco, além disso o documento identificou os principais desafios da segurança cibernética no país e os dividiu em sete campos de ação (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 do que a identificação dos desafios. Um ponto importante no caso brasileiro na identificação dos desafios foram os "Levantamentos de Governança de TI", realizados pelo Tribunal de Contas da União - TCU (BRASIL 2010, 2012, 2014, 2016), o documento teve como objetivo avaliar a situação de governança de tecnologia da informação (TI) na Administração Pública Federal (TCU, 2016). Foram identificados diversos pontos de melhoria a partir das respostas dos agentes públicos, entretanto ainda está distante do ideal, haja vista o nível de adoção insuficiente de muitas práticas fundamentais para que a TI agregue o valor devido aos resultados organizacionais (VIANNA; FERNANDES, 2015).

Assim sendo, a maioria dos documentos analisados apresentaram diversos pontos convergentes sobre os condicionantes da segurança cibernética, separou-se os principais temas em sete grades campos a serem discutidos, com o objetivo de mapear os condicionantes no caso brasileiro:

2.5.1 Estruturas e Processos

As estruturas e processos são pontos fundamentais dentro da área da segurança cibernética. Assim sendo, por essa relevância, diversos condicionantes são encontrados dentro dos campos citados. A heterogeneidade de estruturas e processos é o ponto fundamental a ser discutido hodiernamente, pois os procedimentos globais de cibersegurança não foram definidos formalmente até o momento. Portanto, é necessário definir processos e estruturas que permitam a eficiência da segurança cibernética desde os níveis operacionais até os níveis estratégicos (KAPONIG, 2020).

Em meio a um cenário de heterogêneo acerca da estruturação global da segurança cibernética, os esforços diplomáticos bem sucedidos impulsionados pelo Estado continuam a ser limitados, e muitos dos esforços existentes são ofuscados ou minados por conflitos de interesses nacionais, desconfiança recíproca e/ou disputas geopolíticas que se estendem de outras áreas temáticas (TANCZER; BRASS; CARR, 2018).

Em 2015, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), lançou o relatório *Recommendation on Digital Security Risk Management*. O relatório busca guiar os Estados em como proteger suas infraestruturas e processos críticos de ataques digitais em harmonia com direitos fundamentais. O documento orienta sobre a necessidade de os países adotarem uma estrutura abrangente para gerenciar a segurança cibernética. Ademais, a estrutura e as políticas de implementação devem ser transparentes para promover a confiança nas atividades e no comportamento do governo, inclusive com respeito à divulgação responsável das vulnerabilidades de segurança digital que identificaram, e medidas de mitigação relacionadas (OCDE, 2015). Assim sendo, o ponto fundamental do relatório relacionado às estruturas e processos é sobre a criação ou manutenção de órgãos nacionais competentes a segurança cibernética:

> Garantir o estabelecimento de uma ou mais equipes de resposta a incidentes de segurança informática (CSIRT), também conhecida como Equipe de Resposta a Emergências Informáticas (CERT), a nível nacional e, quando apropriado, incentivar o surgimento de CSIRTs públicos e privados trabalhando colaborativamente, inclusive além das fronteiras. (OCDE, 2015, p.7)

No Brasil, a segurança cibernética encontra-se sob responsabilidade do Gabinete de Segurança Institucional da Presidência da República (GSIPR), o mesmo coordena o 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 segurança cibernética no país. Assim sendo, a dimensão e a assimetria da estrutura de SegCiber do país representa importante desafio a ser enfrentado pelo Brasil (BRASIL, 2015).

Evidencia-se, assim, os vários 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 segurança cibernética. Somados à carência do estabelecimento de governança efetiva da SIC e da SegCiber, e da segurança dos ativos de informação críticos (BRASIL, 2015).

Portanto, os incentivos acerca da criação de órgãos como CSIRTs e CERTs são essenciais, o apoio a esses órgãos é um grande desafio na área, pois os centros de resposta e as redes que eles constroem são responsáveis por incidentes de gerenciamento da segurança global são essencialmente a espinha dorsal da infraestrutura digital de cada país hoje (TANCZER; BRASS; CARR, 2018).

2.5.2 Governança

A governança pode ser definida como na definição de critérios para a tomada de decisões, estabelecimento de regras, responsabilidades e limites da autonomia e ações das partes envolvidas (ROTH; DRESLER, 2012). A governança, também passa pelos padrões desejados de atuação da boa gestão pública passam pela prestação de bens e serviços públicos de qualidade, de forma eficiente, transparente e sustentável (CORREIA; SANTOS; BILHIM, 2017). A governança da segurança cibernética inclui as instituições, iniciativas, políticas, programas e entre outros mecanismos (formais e informais) que integram um ecossistema de competências e responsabilidades distribuídas para a segurança cibernética (HUREL, 2021).

Esse tópico é recente, mas muito relevante, e está sendo explorado em todo o mundo. No Equador, por exemplo, existe uma clara necessidade de implementar uma abordagem estratégica no país, para, assim, propor um modelo de governança da segurança cibernética no país. A intervenção, gestão e avaliação são características do modelo necessário para controlar a segurança da informação nos processos, sistemas e infraestruturas dos quais o Equador depende para sua economia e desenvolvimento (BORBÚA; CHICANGO; HERRERA, 2017). Definir postura de risco, equilibrar requisitos globais e locais, gerenciar dados, responder a mudanças e aplicar métricas relevantes são exemplos de ações de governança da segurança cibernética (EUGEN; PETRUT, 2018). Na Coreia do Sul, existem áreas da segurança cibernética que podem ser realizadas pelo setor privado, e que, para exista uma exemplar governança da segurança cibernética, deve existir medidas de governança conjunta com o setor privado, e não através de ações unilaterais tomadas pelo Estado (PARK *et al*., 2018).

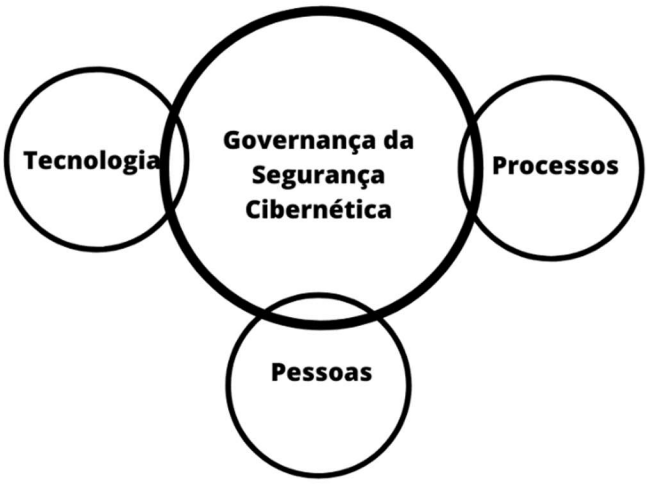

Figura 4: Visão holística sobre a GSC

Fonte: Autor

A Figura 3 representa a estrutura da governança cibernética, uma visão holística e integrada entre as pessoas: organizações e usuários, os processos: políticas internas e externas, integração estratégica, e a tecnologia: softwares especializados para identificar, avaliar, detectar e mitigar os riscos de segurança cibernética.

A governança é um conjunto de processos de gestão elementar para alinhar o planejamento de uma organização às suas ações estratégicas, assim melhora a utilização dos recursos, eleva a qualidade dos serviços prestados e permite a condução exitosa de projetos e de processos. Em segurança cibernética, a governança recebe ainda mais relevância devido à quantidade de atores e setores presentes em todos os processos (BRASIL, 2020). A governança da segurança cibernética "inclui as instituições, iniciativas, políticas, programas e entre outros mecanismos (formais e informais) que integram um ecossistema de competências e responsabilidades distribuídas para a segurança cibernética" (HUREL, 2021).

No Brasil, a E-Ciber é um marco na governança da segurança cibernética, com sua visão holística e integrada "é um componente essencial para o estabelecimento de uma visão e estrutura de governança para um país, bem como para a expansão de novos horizontes para

desenvolvimento de capacidades.” (HUREL, 2021) o documento cita a complexidade da governança:

> A governança na área cibernética está relacionada às ações, aos mecanismos e às medidas a serem adotados com o fim de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais, e acompanhar o desempenho e avaliar os resultados dos esforços empreendidos nesse campo. Essa governança visa incorporar elevados padrões de conduta em segurança cibernética, e orientar as ações de agentes públicos e de agentes privados, ao considerar o papel que exercem em suas organizações, conforme a finalidade e a natureza de seu negócio. Inclui, ainda, o planejamento voltado à execução de programas, de projetos e de processos, e o estabelecimento de diretrizes que irão nortear a gestão de riscos. Nesse contexto, orienta pessoas e organizações quanto à observância das normas, dos requisitos e dos procedimentos existentes em segurança cibernética. (BRASIL, 2021)

A governança da segurança cibernética, portanto, apresenta-se essencial como campo de discussão na área estratégica do governo brasileiro. Se comparado aos demais países desenvolvidos, o Brasil ainda inicia sua caminhada mediante a garantia da proteção do ambiente cibernético. A estrutura de governança deve ser centralizada, com leis, infraestrutura e investimentos, porém, hoje, várias instituições respondem pelo tema, consequentemente dificulta ações coordenadas de longo prazo (VIEIRA; BARRETO, 2019).

2.5.3 Proteção de Infraestruturas Críticas

A proteção das infraestruturas tecnológicas que asseguram serviços essenciais se tornou uma prioridade para a os serviços essenciais tornaram-se uma prioridade para diferentes nações e organizações, considerando a dependência a dependência deles, que está a aumentar exponencialmente de ano para ano (GOMEZ; PARRA, 2017). As infraestruturas críticas são vitais para toda economia nacional (JARMAKIEWICZ; PAROBCZAK; MASLANKA, 2017). Portanto, gigantescos são os prejuízos para um país quando uma dessas infraestruturas são atacadas.

O tema segurança cibernética se destaca como uma função estratégica de governo, e essencial à manutenção e preservação das infraestruturas críticas de um país (MANDARINO JÚNIOR; CANONGIA, 2010). Logo, tais infraestruturas têm sido alvo de constantes ataques cibernéticos, exemplos de órgãos como instituições financeiras, indústrias petrolíferas, instalações de energia nuclear, rede de energia elétrica e a estrutura de comunicação (WILLETT, 2019). Assim sendo, com a dependência cada vez maior desses ativos e serviços

perante os sistemas de informação é, portanto, uma prioridade máxima construir e melhorar a resiliência a ameaças dos sistemas de informação (KAPONIG, 2020).

.

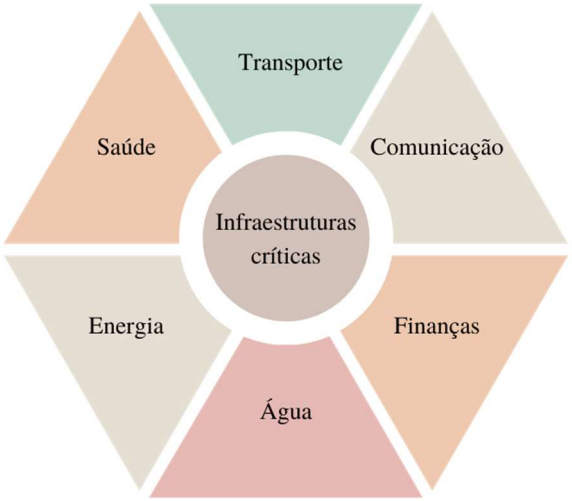

Figura 5: Prisma das infraestruturas críticas

Fonte: Autor

Em 2018, o governo brasileiro publicou o decreto nº 9.573, que estabeleceu a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), que tem por finalidade "garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços" (BRASIL, 2018a, p. 1). Além de definir as infraestruturas críticas para o governo brasileiro, como "instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2018a, p. 1). O documento explora a importância da proteção dessas infraestruturas, e estabelece que são necessárias diretrizes e instrumentos para salvaguardar as infraestruturas críticas consideradas indispensáveis à segurança nacional. Portanto, a publicação do decreto, representou a atenção do governo para o tema, pois a proteção das infraestruturas críticas tornou-se elementar e uma questão estratégica por demandar ações que resguardem serviços básicos de uma sociedade.

2.5.4 Legislação

Diversas mudanças sociais e organizacionais ocorreram nas últimas décadas com o advento da tecnologia. Fatores organizacionais, tais como comunicação, cultura de segurança, política e estrutura organizacional, estão entre os motivos mais proeminentes para o comprometimento da segurança cibernética (SOOMRO; SHAH; AHMED, 2016). Logo, a legislação se tornou, também, fator de mudança. Pois, diversos são os benefícios trazidos pela tecnologia, entretanto, também malefícios como ataques e crimes cibernéticos alcançaram a sociedade. Os autores destas ameaças podem ser indivíduos, grupos de crime organizado ou inteligência estrangeira (DYGNATOWSKI; DYGNATOWSKI, 2020). Portanto, a normatização da segurança cibernética, transformou-se em um desafio relevante para os governos de todo o planeta. Pois, faz-se necessário a criação de leis eficazes alinhadas a estratégia de segurança nacional.

> A legislação concentra-se em dois aspectos. Primeiro, ela faz arranjos institucionais de segurança cibernética. Ela estabelece e melhora os sistemas relevantes de segurança de equipamentos de rede, segurança de sistemas de rede, segurança da informação em rede, e assim por diante. Também fortalece a proteção de informações pessoais, ao apresentar as disposições do nome real da rede e do controle da rede. Em segundo lugar, a legislação estipula as obrigações legais do operador de rede, produto de rede, provedor de serviços, participante de rede, supervisão de rede, e as responsabilidades legais do comportamento ilegal (GUO, 2018, p.141).

A segurança cibernética é um tema transversal, multidisciplinar e multissetorial, a temática, por conseguinte, é abordada em diversos normativos no Brasil, sob diversos enfoques e competências (BRASIL, 2021). O arcabouço normativo, mesmo que em processo de desenvolvimento, o respectivo nível de maturidade ainda encontra-se em patamar aquém do desejado nos órgãos e entidades da APF (BRASIL, 2015), o governo brasileiro apresentou alguns documentos na área como a publicação do O Livro Verde: Segurança Cibernética no Brasil (MANDARINO JR.; CANONGIA, 2010), elaborado em 2010, que aponta potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, já a Lei nº 13709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD), publicada em 2018, trouxe importantes disposições acerca da proteção de dados pessoais e alterações no texto da Lei nº 12.965 de 23 de abril de 2014, considerada como o Marco Civil da Internet. Por fim, em 2021 o governo brasileiro publicou o decreto nº 10.222, contendo a Estratégia Nacional de Segurança Cibernética - E-Ciber, com as principais orientações sobre as ações pretendidas pelo

governo, em termos nacionais e internacionais, na área da segurança cibernética (BRASIL, 2021).

> Ainda no caso do Brasil, este tem história na sociedade da informação, e no campo da segurança da informação e comunicações tem governança estabelecida, legislação vigente, vem construindo seu arcabouço normativo no âmbito do governo federal, e apesar de recente, se comparado ao arcabouço de leis, normas, padrões dos países desenvolvidos, tem destaque de atuação e reconhecimento nacional e internacional de sua competência em temas diretamente correlacionados à segurança cibernética. Vale aqui destacar, a competência técnica nacional de tratamento e resposta a incidentes de redes computacionais de governo, (o que significa, em resumo, ações de segurança contra ataques dos chamados malwares), reconhecida em nível nacional e internacional (MANDARINO JÚNIOR; CANONGIA, 2010, p.37).

2.5.5 Sensibilização e Capacitação

A sensibilização e capacitação de gestores e da sociedade em geral acerca do tema segurança cibernética é um grande desafio hodiernamente. A interação e o envolvimento de parceiros civis, públicos e privados, é essencial para a criação de uma consciência pública sobre a segurança cibernética. Esse tipo de instrução promove a cultura da segurança cibernética (JUNIOR; STREIT, 2017). Já 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 segurança cibernética (NORRIS *et al*., 2019). Toda a sociedade deve ser sensibilizada sobre a segurança cibernética, a fim de aumentar a consciência, o interesse pessoal e a atenção sobre o tema. Essas medidas de conscientização ajudarão a criar uma compreensão da necessidade de garantir, promover e criar uma cultura da segurança cibernética (KAPONIG, 2020).

O desenvolvimento dessa cultura pode ser iniciado já na educação básica, com programas de sensibilização dentro das escolas, sobre a importância da proteção dos dados, até nas universidades com acordos de cooperação técnica, entre as mesmas e empresas privadas, que podem ser realizados para o desenvolvimento de tecnologias de suporte ao setor cibernético, além de programas de capacitação que podem ser disponibilizados aos alunos (JUNIOR; STREIT, 2017). Outro ponto essencial, é a capacitação adicional dos gestores da área da segurança cibernético, eles devem ser capazes reconhecer incidentes cibernéticos e detectar anomalias nos seus sistemas (KAPONIG, 2020).

A falta de programas de sensibilização, capacitação, investimentos e formação de

longo prazo, no governo brasileiro, contribuem para o aumento de vulnerabilidades. Assim sendo, o governo brasileiro destaca que as organizações, públicas e privadas, estabeleçam políticas e procedimentos de segurança cibernética além da necessidade de capacitação contínua e estruturada para todos os colaboradores, por meio de programas de capacitação (BRASIL, 2020).

2.5.6 Gestão de Risco

A gestão de riscos é função crucial para uma melhor governança e, é a pedra fundamental da defesa de uma organização. Além de ser o ponto de partida de medidas de controle proporcionais, eficientes e efetivas para mitigar os riscos identificados (OCDE, 2015). O TCU (2018) define a gestão de riscos corporativos como uma atividade que visa identificar, mensurar, classificar, tratar e monitorar os riscos de forma planejada, estruturada e integrada, de modo que a entidade possa atingir seus objetivos. Já a Associação Brasileira de Normas Técnicas afirma que "A gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos." (ABNT, p.5, 2009).

No caso da segurança cibernética, a gestão de riscos é fundamental para quaisquer organizações, uma vez que a proteção absoluta dos sistemas de segurança não é realista. Consequentemente, a necessidade de sistemas cada vez mais complexos nos países e organizações torna-se necessários devido as constantes ameaças cibernéticas. Tais ataques podem violar as bases dos sistemas de informação. Por exemplo, a violação de dados afeta principalmente a confidencialidade, a negação de serviço e os ataques de resgate envolvem a disponibilidade de informações, e a desfiguração do site reduz a integridade, enquanto os ataques de *phishing* podem afetar tanto a confidencialidade quanto a integridade (MCSHANE; NGUYEN, 2020).

A gestão de riscos cibernéticos precisa tratar dos aspectos técnicos e humanos de forma holística (LEE, 2021). Além de ser um processo contínuo de manter o efetivo funcionamento dos ativos críticos das organizações em qualquer circunstância (KURE; ISLAM, 2019). Assim torna-se um condicionante para as organizações gerenciar os riscos cibernéticos devido à complexidade de todos os processos envolvidos, o que envolve a identificação dos riscos e vulnerabilidades, além da aplicação de ações administrativas e

soluções para garantir que a organização esteja adequadamente protegida “uma das etapas críticas do gerenciamento de risco é entender as vulnerabilidades e ameaças que possam representar quaisquer riscos potenciais. Este papel contribui para essa direção e se concentra em três grandes aspectos de gerenciamento de risco, ou seja, identificação de ativos, vulnerabilidade, e avaliação de ameaças e identificação de riscos.” (KURE; ISLAM, p.340, 2019).

2.5.7 Cooperação Internacional

A internet está crescendo e se tornando cada vez mais ampla e disponível. Porém, mesmo com todos os benefícios trazidos pelo desenvolvimento da internet, o ciberespaço, também, está se tornando a fonte do mau uso, e competir com o crime cibernético requer uma cooperação internacional (PROTRKA; MARIC; PLECAS, 2017). A cooperação internacional é fundamental para o aperfeiçoamento das diretrizes e ações da segurança cibernética. Entretanto, apesar de quase três décadas de esforços diplomáticos, colaboração transversal e atenção acadêmica, a cooperação internacional da segurança cibernética tem sido lenta e incerta (CARR, 2016). Sendo assim a cooperação internacional é um relevante condicionante na área da segurança cibernética.

A diferença no entendimento de cada país sobre o que é a segurança cibernética é uma das principais razões que alimentam o impasse que prejudica as discussões sobre segurança cibernética produtiva e a produção de normas a nível internacional (URGESSA, 2020). Já Souza Junior e Streit (2017), afirmam que a cooperação deve ser baseada em uma relação de confiança.

> Assim a cooperação entre nações é cada vez mais necessária para dar tração a discussões sobre governança cibernética global, visando a conclusão de acordos capazes de estabelecer assistência mútua para garantir a inclusão digital, para compartilhamento de informações e colaboração nas investigações de cibercrimes, bem como para a harmonização e garantia de aplicação independentemente dos limites territoriais impostos por modelos regulatórios tradicionais (Bechara; Schuch, p.360 2021)

Ou seja, é necessária cada nação deixar de lado suas inseguranças e desacordos e começar a cooperar para a criação de um espaço cibernético mais seguro, a partir de acordos

internacionais, compartilhamento de informações e uma cooperação global (KOSTYUK, 2014).

3. MÉTODOS E TÉCNICAS DE PESQUISA

Nesta seção serão apresentados os métodos e técnicas de pesquisa utilizados na pesquisa para alcançar os objetivos pré estabelecidos.

3.1 Tipologia e descrição geral dos métodos de pesquisa

O trabalho apresentado tem sua natureza aplicada, com o objetivo exploratório e descritivo, além de que trata-se de uma pesquisa qualitativa que, busca mapear os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI. A pesquisa qualitativa é adequada para compreender a complexidade dos fenômenos sociais por meio da análise e busca dos significados contidos nas ações e informações advindas das pessoas que participam do estudo (TRIVIÑOS, 1987).

Inicialmente, apresentou-se uma revisão de literatura acerca da segurança cibernética, explorou-se desde os conceitos iniciais sobre sua importância, das vulnerabilidades presentes nas organizações, até temas mais complexos como a proteção das infraestruturas críticas de cada país. Assim, baseado em artigos anteriores, separou-se em sete grandes temas a serem abordados por meio de entrevista semiestruturada aplicada a gestores da segurança da informação presentes na área pública brasileira.

Algumas das principais vantagens em se utilizar a entrevista estruturada, e na sua rapidez e no fato de não exigirem exaustiva preparação dos pesquisadores, o que implica em custos relativamente baixos (GIL, 2009). A entrevista semiestruturada, também, constitui num dos principais meios que o investigador possui para realizar a coleta de dados, oferecendo perspectivas possíveis para que o entrevistado alcance a espontaneidade, assim, enriquecendo a investigação (TRIVIÑOS, 1987).

3.2 Entrevistados

Para realizar a entrevista semiestruturada optou-se por selecionar participantes que possuem função na área pública, uma vez que o objetivo da pesquisa é mapear os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI . Outro critério elementar foi a escolha de participantes que tenham experiência da área da segurança cibernética, para assim o mapeamento dos condicionantes ser mais claro a partir das respostas dos entrevistados devido a experiência que os mesmos possuem na área. Foram realizadas 9 entrevistas *online* com indivíduos de organizações públicas dos poderes executivo, legislativo e judiciário.

3.3 Procedimento de coleta e análise dos dados

As entrevistas foram realizadas com o objetivo de mapear os principais condicionantes encontrados pelos gestores públicos com a segurança cibernética. As perguntas previamente elaboradas, baseadas na revisão de literatura, tiveram como objetivo entender as experiências de cada gestor com a segurança cibernética na área pública federal do Brasil (Apêndice 1).

Desenvolveu-se um roteiro com quinze questões abertas com o objetivo de o entrevistado apresentar suas experiências e percepções acerca da segurança cibernética na área pública do Brasil. As perguntas foram baseadas nos sete grandes temas anteriormente explorados na revisão de literatura. As entrevistas foram realizadas entre março e abril de 2022 e tiveram duração média de 40 minutos.

O plano de realização de entrevistas individuais além da confidencialidade em relação a identificação dos entrevistados mostrou-se eficaz em proporcioná-los conforto e abertura suficientes para compartilhar suas experiências, reduzindo, assim a probabilidade de viés nas respostas. Outro ponto a ser destacado é que ao longo da entrevista, devido ao conhecimento prévio e fluidez das conversas, permitiu que outras perguntas também fossem realizadas.

Na análise prévia das transcrições, 118 pequenas partes das entrevistas foram evidenciadas e listadas por representar, de alguma maneira, dificuldades que os gestores possuíam em relação à segurança cibernética. Posteriormente, na etapa de exploração do material, estes trechos foram classificados de acordo com os temas explorados, e agrupados por possuírem relação e, os trechos que tratavam de uma mesma situação, consolidados em sentenças únicas. Desta segunda etapa foram obtidos 50 itens que foram agrupadas em 9 construtos que representam os condicionantes encontrados pelos gestores, definidos conforme o julgamento do pesquisador com base nas impressões observadas ao longo das entrevistas.

Escolheu-se a análise de conteúdo como a técnica mais adequada para análise dos dados, que por meio de procedimentos sistemáticos permite inferir conhecimento dos discursos analisados seguindo as etapas propostas em Bardin (2016): (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 condicionantes relacionados à segurança cibernética área pública federal do Brasil. 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 e reflexão.

4. RESULTADOS E DISCUSSÃO

4.1 Infraestrutura

Segundo os relatos coletados, a área pública possui grandes deficiências na parte infraestrutural de segurança cibernética. Os gestores afirmaram que os equipamentos e softwares utilizados são defasados, além dos procedimentos não serem adequadas para a defesa de constantes ataques que os órgãos públicos sofrem. Tais afirmações podem ser exemplificadas nas respostas abaixo:

> *Não possuímos os equipamentos adequados. Primeiro porque a gente não tem domínio do mundo de fora e que mal tem o domínio do mundo de dentro e a complexidade que é um ambiente de TI, por exemplo, é muito grande.*

> *Existe uma vulnerabilidade tal qual o domínio de quem está dentro do mundo dos órgãos públicos, devido a defasagem dos equipamentos, caso acontece um ataque sofisticado é muito difícil antecipar e bloquear. É um complexo altamente desafiador.*

> *A gente tem tido até alguma evolução de compra de equipamentos, mas as pessoas esquecem que equipamento não se administra e eles não fazem as defesas funcionarem sozinhas. E a gente precisa de pessoas de processos bem sólidos e padronizados.*

> *Eu acho que está muito atrás assim. A gente tem órgãos sem antivírus, órgãos que, por vezes não têm investimento. E acaba que assim, em termos de equipamento, eu acho que a gente está muito precário. Até porque muitas vezes o gestor não tem nem dinheiro para investir em todos os equipamentos, deixar todos atualizados, o que gera enormes vulnerabilidades.*

> *"Esbarramos em situações como processo de aquisição, que geralmente é um processo moroso, burocrático, por conta de todo o processo licitatório"*

Segundo esses relatos, é recorrente que a existência de equipamentos ultrapassados é um grande desafio para a área pública brasileira. Ou seja, investimentos na parte estrutural são essenciais, para a evolução da segurança cibernética no país e tornar a segurança como parte elementar em todos os órgãos. Outro ponto a ser destacados são os processos, os gestores majoritariamente afirmaram que falta o foco em prevenção, e que na maioria das vezes, a parte mais alta na hierarquia enxerga o setor de TI apenas quando existe algum problema, ou quando são atacados, assim sendo, o trabalho preventivo é desconsiderado.

> *Muitas ações que precisariam estão sendo montadas hoje para que no futuro não houvesse problema deixam de serem colocadas em prática porque a cobrança atual é mais importante e tem mais valor para a instituição.*

> *Hoje eu acho que a gente não tem muito foco em prevenção. A gente tenta não ser invadido, mas na minha visão, estamos sempre suscetíveis a invasões.*

Assim sendo, as afirmações apresentadas foram agrupadas para formar o construto "infraestrutura" que reflete os condicionantes infraestruturais sobre a segurança cibernética na área pública brasileira. Desta análise resultaram seis itens apresentados no Quadro 1.

Quadro 1 - Construto Infraestrutura

CONSTRUTO 1: Infraestrutura Parte infraestrutural sobre a segurança cibernética na área pública do Brasil.
1. Os equipamentos são defasados
2. Faltam investimentos em *softwares* adequados
3. A burocracia impede a aquisição de equipamentos
3. Processos sólidos e padronizados são necessários
4. A área de TI deve ser vista como parte elementar nos órgãos
5. Softwares desatualizados geram diversas vulnerabilidades
6. A infraestrutura de TI não é adequada

Fonte: Elaborado pelo autor.

Pela sua relevância, o setor público federal constantemente será 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 falta de infraestrutura de TI adequada torna-se um grande desafio uma vez que é fundamental existir na organização uma infraestrutura adequada para a manipulação dos dados e do bom funcionamento do órgão (SOUSA, 2013). Ou seja, a falta dessa estruturação torna os órgãos da administração pública brasileira vulneráveis a ataques conforme elencando na revisão de literatura.

4.2 Estrutura

De acordo com a revisão de literatura realizada, uma das questões principais levantada pelos autores é que não existe um órgão específico para coordenar e fomentar o compartilhamento de boas práticas sobre a segurança cibernética no Brasil. O Gabinete de Segurança Institucional emite portarias que não são operacionais segundo alguns gestores, e que uma agência específica para fazer essa coordenação seria essencial, pode-se exemplificar tal opinião, segundo as respostas abaixo:

> *Então, sim, deveria existir algum órgão com atribuição exclusiva. Se pudesse se dedicar somente a Segurança Cibernética e com autonomia também [...]. Então, acho que seria fundamental que se tivesse, sim, talvez uma agência[...]. O trabalho do GSI tem uma abrangência pequena, apesar de que eles fazem um bom trabalho com os recursos que se tem, porém acredito que falta de autonomia.*

> *Eu tenho certeza de que a ausência de um órgão assim é um fator que gera futuros impactos. Se você observar o Executivo, por exemplo, que normalmente é o grande demandante o Judiciário e o Legislativo como um segundo patamar para quando o Executivo estabelece uma estratégia nacional de governo eletrônico, estratégia nacional e de serviço aberto etc. E nessa estratégia ela deixa uma lacuna forte sobre os riscos que isso impacta no próprio serviço. Portanto percebe-se que a segurança cibernética fica em segundo plano só se torna o primeiro plano no momento que há um problema.*

> *Acho que deveria ter uma agência de segurança da informação específica, como se fosse a NSA americana para trabalhar do lado da ANPD. Acho improvável de isso acontecer no cenário brasileiro, mas acho que é muito relevante.*

> *. Então, acho que sim. Seria muito positivo essa iniciativa. E, se possível, passando em todas as esferas. Eu não sei como isso poderia ser aplicado na prática, mas você ter um órgão mais de alto nível dando diretrizes para essas questões seria muito bom.*

Porém outros gestores não acreditam que a criação de um novo órgão vai trazer grandes benefícios, segundo eles, aumentaria ainda mais a burocracia existente e não teria sentido, uma vez que a atribuição de coordenação é realizada pelo GSI. Pode-se observar nas afirmações abaixo:

> *A gente vê pelo modelo de outros países que é comum ter isso. Alguma agência que faça mais sugestões e orientações. Então, por exemplo, existe o NIST tem uma ligação muito grande com o governo norte-americano. Mas talvez a gente acabe meio que reinventando a roda ao criar uma agência desse tipo, porque já existem muitos frameworks no mundo. Então talvez eu não tenho certeza se isso teria um ganho muito grande tirar essa função do GSI hoje e colocando uma outra agência.*

Portanto percebe-se que existe uma discordância de ideais entre os gestores sobre o tema, o que se apresenta como um ponto importante de discussão sobre a necessidade da criação de um novo órgão que coordene a segurança cibernética no país. Sendo assim, as respostas foram classificadas e agrupadas para formar o construto "Estrutura":

Quadro 2 - Construto Estrutura

CONSTRUTO 2: Estrutura Necessidade da criação de um órgão central que coordene a segurança cibernética no país
7. As portarias do GSI não são operacionais
8. O trabalho do GSI tem abrangência pequena
9. O GSI não possui a autonomia necessária para a coordenação
10. Diretrizes mais operacionais são necessárias
11. Não existe um padrão de parâmetros de controle e metodologias entre os órgãos
12. Não existe um órgão resposável pelo compoartilhamento de boas práticas entre os órgãos

Fonte: Elaborado pelo autor.

A estrutura da segurança cibernética no Brasil é ponto de grande discussão. Os autores Souza e Almeida (2016) afirmam que o Estado brasileiro possui uma estrutura basilar pronta para atuar nas áreas de segurança e defesa cibernética, ainda que em desenvolvimento, perante os condicionantes presentes, entretanto a maioria dos gestores afirmaram que a estrutura atual não é adequada e que a criação de um órgão central que coordenasse a segurança cibernética no país seria essencial. Isso demonstra discordância entre a literatura e a realidade relatada pelos os gestores.

4.3 Governança

A governança da segurança cibernética é ponto fundamental em qualquer instituição, e na área pública não é diferente, os processos e as tomadas de decisão devem ter a segurança como aspecto elementar. Segundo os gestores, existe um grande desafio na governança da segurança cibernética da área pública, a grande maioria deles afirmam que as áreas mais estratégicas não se importam como deveriam com a segurança da informação:

> *A gente não tem governança. A gente não estaria falando segurança cibernética se não fosse para a gente proteger dados e proteger informações importantes. Precisamos evoluir para uma governança maior e aí olhando a governança como expectativa do que é uma organização que tem sobre as suas unidades a importância da segurança cibernética, além de todas as unidades tratarem melhor os dados, administrar melhor, e gerenciar melhor o ciclo de vida dos dados.*

> *Eu diria que a gente está a evoluir muito nesse aspecto de governança. Infelizmente não é como deveria ser feito [...]. A governança em si, ela é muito incipiente. Aqui, as áreas de gestão avaliam os nomes oferecidos e propõem para as instâncias de governança que se faça algumas coisas. Então a gente tem buscado tentar cobrir essa lacuna. O pessoal planeja estratégias para a área, mas eu entendo que ela ainda tem esse problema porque não existe as instâncias de governança por si só. Deveriam existir instâncias de governança.*

> *Tem que melhorar muito. Ela está ocorrendo aos trancos e barrancos e não está ocorrendo aqui. Mas ela vem de baixo para cima e não de cima para baixo, que é como deveria ser.*

Percebe-se, portanto, a partir das afirmações a dificuldade de relacionamento entre as áreas mais estratégicas com a parte operacional relacionado a segurança cibernética. Segundo os entrevistados, o planejamento e as medidas elaboradas realizadas não são exemplos de uma governança efetiva, apresentando diversas lacunas, dentre elas a governança acontecendo da parte operacional para atingir a parte mais estratégica, uma vez que a última não demonstra dar relevância a governança da segurança cibernética. A partir das respostas, as afirmações foram agrupadas e classificadas para formar o construto "Governança".

Quadro 3 – Construto Governança

CONSTRUTO 3: Governança Conjunto de práticas, padrões assumidos, com o objetivo de garantir controles efetivos, ampliar os processos de segurança e desempenho.
13. Áreas estratégicas não enxergam a SegCiber como ponto elementar 14. A governança é incipiente 15. O controle de processos de TI internos não são efetivos 16. Deveriam existir instâncias de governança 17. A maioria dos órgãos não possuem uma política específica ou modelo de governança da segurança cibernética

Fonte: Elaborado pelo autor.

A governança é um conjunto de processos de gestão elementar para alinhar o planejamento de uma organização às suas ações estratégicas (BRASIL, 2020). Assim sendo pode-se inferir pelas respostas dos gestores que esse alinhamento não é realizado uma vez que área da segurança cibernética não é tratada com a devida relevância.

4.4 Ataques cibernéticos e credibilidade

Foi questionado aos entrevistados, quais eram os maiores condicionantes do setor de segurança cibernética perante as vulnerabilidades que a instituição deles possui. A resposta mais recorrente foi a preocupação com os ataques cibernéticos, segundo eles, o maior problema que poderia ocorrer seria sofrer ataques e, consequentemente ocorrer a perda de credibilidade do órgão diante da sociedade, isso pode ser exemplificado pelas respostas a seguir:

> *É tudo interligado. Eu acho que assim que a gente sofrer ataques, isso vai prejudicar a imagem da instituição e com isso a gente tenta ter os mecanismos possíveis da gente, minimizar isso, mitigar esses ataques.*

> *Hoje eu diria que a nossa maior preocupação é imagem da instituição.*
>
> *As nossas maiores preocupações são com os ataques cibernéticos. Acho que eu apostaria que essa é a melhor preocupação de todos*
>
> *Então, eu diria que o principal desafio e a principal preocupação do órgão é contra ataques de grupos mais avançados, que tenham a intenção de realizar ações de espionagem para obtenção de dados e de informações.*

Assim sendo, entende-se a partir das respostas que a maior preocupação dos gestores de TI da área pública é com os ataques cibernéticos. Outro ponto de atenção é com a imagem de instituição, existe um enorme cuidado em zelar pela imagem dos órgãos e transparecer segurança. Portanto, separou-se as argumentações que possuíam pontos em comum para formar o construto "Ataques cibernéticos e credibilidade"

Quadro 4 – Construto Ataques cibernéticos e credibilidade

CONSTRUTO 4: Ataques cibernéticos e credibilidade Preocupação dos órgãos públicos com os ataques cibernéticos e com a credibilidade do órgão junto à sociedade
18. Os ataques cibernéticos sofridos tem foco em obter dados 19. Os ataques cibernéticos são comuns 20. Existe uma grande preocupação com a imagem dos orgãos 21. Os orgãos devem demonstrar que tem a capacidade de serem protegidos 22. Existem protocolos para mitigar os riscos dos ataques

Fonte: Elaborado pelo autor.

A tendência é que os ataques cibernéticos a órgãos públicos se tornem cada vez mais sofisticados (PAIVA, 2020). O que leva a uma grande preocupação dos gestores conforme suas respostas, uma vez que, segundo eles é muito difícil mitigar os ataques com as ferramentas que possuem. Além de que os ataques podem afetar a credibilidade do órgão diante da sociedade.

4.5 Cultura

Um grande desafio apontado pelos gestores é a necessidade de uma mudança cultural nas organizações públicas. Segundo os entrevistados, ainda existe a ideia entre os colaboradores em geral que a parte de segurança da cibernética é um setor específico para atividade específicas, assim sendo, não faz parte das funções principais dos órgãos. Ou seja, não dão a devida relevância para a segurança cibernética, isso pode ser exemplificado pelas afirmações a seguir:

> *"Eu mesmo que o maior desafio é a cultura, a grande questão, hoje, é cultural também. Mudar os hábitos, mudar as pessoas e gerar o convencimento de que, de que a segurança cibernética é relevante."*

> *"[...]significa que a segurança cibernética ainda não está na agenda da alta administração como algo prioritário, mas sim como algo secundário, algo que é muito exclusivo, "A TI cuida disso e deixa na mão deles". E é um assunto que perpassa por toda a organização."*

> *"E aí quando o problema aparece de fato precisamos de uma completa mudança cultural. É algo que precisa de uma transformação maior. Não se passa especificamente com tecnologia e práticas."*

Percebe-se, portanto, que existe uma grande resistência das áreas estratégicas em tratar a segurança cibernética como tema prioritário nas suas agendas. Isso, é um fator cultural que prejudica imensamente o desenvolvimento da segurança cibernética 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. As afirmações em comum foram agrupadas e categorizadas para formar o construto "Cultura".

Quadro 5 – Construto Cultura

CONSTRUTO 5: Cultura Conjunto de conhecimentos teóricos e práticos acerca do segurança cibernética
23. Mudança cultural é importante 24. Ainda existe a cultura de que TI é secundária.

25. A mundança de hábitos é necessária em toda administração pública.
26. O ponto de maior vulnerabilidade nas organizações são as pessoas.
27. As áreas estratégicas não enxergam a segurança cibernética como fundamental.
28. A mudança cultura é mais relevante que tecnologias e práticas

Fonte: Elaborado pelo autor.

Os investigadores de segurança cibernética têm defendido consistentemente que é necessário construir uma cultura de cibersegurança é essencial para mudar atitudes, percepções, e incutir bons comportamentos de segurança (VEIGA *et al.,* 2020). Isso vai de encontro com a afirmação dos gestores que alertam sobre a necessidade da criação de uma cultura de segurança cibernética para o desenvolvimento do tema no país, segundo eles uma mudança de ideias, comportamentos e atitudes são necessárias.

4.6 Capacitação e Sensibilização

Foi questionado aos gestores se eles acreditam que os colaboradores de órgãos públicos da área da segurança cibernética possuem a capacitação adequada e se o órgão fornece essa capacitação. Segundo eles, os órgãos fornecem a capacitação adequada, porém, existe uma resistência e liberar verba para cursos específicos, uma vez que os superiores não enxergam a importância do investimento, pode-se exemplificar pelas respostas:

> *"O gestor médio da Esplanada ainda tem uma visão de que gastar, de consumir recurso financeiro para a segurança e formação é gastar dinheiro, e não é isso. Na verdade, é mitigação de risco".*

> *"[...] porque como o gestor não tem consciência proativa de como tratar aquele assunto, acaba que é caro demais gastar num curso, num treinamento, num seminário.*

> *"realmente na administração pública os anos anteriores sempre foi complicado a gente negociar algum recurso para segurança, porque é uma coisa que ninguém vê, só vê quando é atacado."*

Outro ponto que foi destacado é da sensibilização dos gestores, segundo os entrevistados é difícil gerar interesse e engajamento dos colaboradores em geral da importância da segurança cibernética como observa-se pelas afirmações:

> *"Acredito que o principal desafio é acessibilidade dos gestores. Os níveis mais altos, normalmente não são pessoas acessíveis. Muitas vezes a gente fazemos ações de conscientização e capacitação e educação em segurança. Mas quem mais precisava ouvir, muitas vezes não vai lá no auditório ouvir uma palestra"*

> *"Geralmente o usuário não gostava nem que se fale de segurança, porque para ele é um negócio pra atrapalhar o dia-a-dia dele."*

> *. E eu já tive que dar palestra a muita gente. [...] E aí acaba que é difícil até a pessoa se interessar, porque normalmente, quando você ouve de segurança cibernética você que é um usuário médio, você só sabe do hacker que rouba dinheiro no celular, né? Você só ouve falar disso.*

Portanto, a sensibilização dos colaboradores em geral se torna outro grande 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. Posto isto, as afirmações em comum foram agrupadas e categorizadas para formar o construto "Capacitação e Sensibilização".

Quadro 6 – Construto Capacitação e Sensibilização

CONSTRUTO 6: Capacitação e Sensibilização Capacitação e sensibilização dos servidores em geral acerca do tema segurança cibernética
29. Os órgãos não tem capacitação dos gestores de TI como foco 30. Faltam investimentos em cursos mais sofisticados 31. Os gestores das áreas estratégicas não enxergam o gasto em capacitação em segurança cibernética como investimento 32. Falta engajamento dos servdores em geral acerca do tema 33. A acessibilidade dos gestores de níveis mais altos é um grande desafio 34. Os recursos para área de segurança são escassos

Fonte: Elaborado pelo autor.

A capacitação dos funcionários é essencial segundo os gestores afirmaram nas entrevistas. Segundo a literatura, 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 segurança cibernética (NORRIS *et al*., 2019). Ou seja, existe um alinhamento evidente entre o que os gestores afirmaram e a literatura abordada sobre o tema.

4.7 Legislação

A legislação em segurança cibernética 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. Como exemplificado no referencial teórico, no Brasil temos algumas legislações como: a Lei de acesso à informação, LGPD etc. Assim sendo, os entrevistados foram questionados acerca do nível de maturidade e sobre a importância dessas legislações na área pública. Segundo grande parte dos gestores, o nosso arcabouço normativo tem um bom nível de maturidade, porém em certos pontos faltam diretrizes mais operacionais, as legislações atuais são mais estratégicas e muitas vezes não tem efeito prático. Podemos observar isso nas afirmações:

> *"Eu acho que a legislação em si é muito boa. Ela se alinha aí com a legislação da Europa e tudo mais, mais a capacidade dos órgãos de executarem determinadas leis que impedem da lei realmente vigorar e ser efetiva. Falta atingir a parte mais operacional. Na prática, o dia a dia"*

> *"Então, assim, a lei é muito legal, muito boa. Sim, ela regulamenta, tem a disciplina, bem a matéria, mas a prática do dia a dia que não nos permite por ela em prática sempre."*

> *"As leis, as políticas de forma geral, de controles de segurança mais próximos do que a gente temos um arcabouço bacaninha. Não é o melhor dos mundos. Mas a gente está longe de ser precário. Mas comparando com os normativos americanos como do NIST, por exemplo, tem iniciativas que são mais próximas do operacional."*

Observa-se, portanto, que em geral o arcabouço normativo brasileiro tem um bom nível de maturidade, principalmente as diretrizes estratégicas. Porém, segundo os gestores, as leis não são tão efetivas na parte operacional, faltam orientações para os problemas que os gestores encontram dentro das organizações diariamente. A partir das respostas, os argumentos em comum foram agrupados para formar o construto "Legislação".

Quadro 7 – Construto Legislação

CONSTRUTO 7: Legislação Leis, normas e políticas sobre a segurança cibernética presentes no Brasil
35. O arcabouço normativo brasileiro possui um bom nível de maturidade. 36. Faltam legislações operacionais. 37. O Estado está buscando trazer os temas relacionados a segurança cibernética a tona. 38. As legislações tratam de temas muito específos 39. Existem grande lacunas a serem cobertas pela legislação 40. Os gestores são carentes de orientações práticas.

Fonte: Elaborado pelo autor.

Segundo a literatura, o arcabouço normativo, mesmo que em processo de desenvolvimento, o nível de maturidade ainda se encontra em patamar aquém do desejado nos órgãos e entidades da Administração Pública Federal (BRASIL, 2015). Isso vai ao encontro do que os gestores afirmaram, segundo eles, a legislação brasileira ainda está em um nível abaixo do ideal e que normas mais operacionais são extremamente necessárias. Ou seja, é essencial o desenvolvimento de legislações maduras e operacionais para o desenvolvimento do arcabouço normativo brasileiro sobre segurança cibernética.

4.8 E-Ciber

A Estratégia Nacional de Segurança cibernética foi um marco na legislação brasileira acerca do tema segurança cibernética, 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. As respostas foram distintas, alguns gestores afirmaram que a elaboração do documento foi muito relevante, como apresentado nas respostas:

> *"A E-Ciber foi fundamental para alertar sobre a importância da segurança cibernética, para trazer o problema para o patamar mais alto, isso foi importante a meu ver."*

> *"A E-Ciber ajuda a reforçar os movimentos institucionais. Ajuda a justificar investimentos na área. É uma questão mais de estratégia, de adoção de alguma de alguma questão. Você a utiliza como embasamento técnico."*

Porém outra parte dos gestores afirmaram que tiveram o conhecimento da estratégia, entretanto ela não teve efeito prático dentro das instituições. Segundo eles, o documento não tem diretrizes práticas e que corroborem com a realidade das instituições, pode-se observar isso nas afirmações:

> *"Sendo bem sincero, não para órgão em si em alguns pontos, não teve[...]. Mas, em termos de definição da estrutura interna do que o órgão faz para se proteger E-Ciber não foi tão relevante."*

> *"Na prática, a gente não trouxe isso para dentro da organização."*

> *"Mas pelo fato de ser nova, eu acho que. A gente, a gente tem alguns pontos, poderia trabalhar melhor. [...] acho que a aplicação da norma, ela fica um pouco complexa para os alunos menos maduros."*

Isto posto, observa-se que a E-Ciber mostrou-se um documento importante para a segurança cibernética brasileira, porém as diretrizes propostas foram criticadas pelos gestores, faltam orientações mais práticas no seu desenvolvimento o que, consequentemente, a afasta da realidade das instituições, desta forma as afirmações em comum foram agrupadas e categorizadas para formar o construto "E-Ciber".

Quadro 8 – Construto E-Ciber

CONSTRUTO 8: E-Ciber Estratégia Nacional de Segurança Cibernética
41. A E-Ciber foi um importante documento para o desenvolimento da Segurança Cibernética no Brasil. 42. Ajuda a justificar investimentos na área.

43. Diretrizes não são operacionais.
44. Diretrizes afastam a estratégia da realidade das instiuições.
45. Existem gestores que não tiveram conhecimento da estratégia.
46. Poucos órgãos colocaram as diretrizes em prática.

Fonte: Elaborado pelo autor.

Como afirmado na seção anterior os normativos brasileiros estão aquém do nível desejado, um grande exemplo é a E-Ciber, um decreto tão relevante para área e alguns gestores não sabiam da sua existência, isso demonstra a falta de alinhamento entre a legislação e a realidade dos gestores. Além de afirmarem que a estratégia não possui diretrizes operacionais, o que foi citado diversas vezes.

4.9 Cooperação internacional

A cooperação internacional sobre a segurança cibernética é um tema complexo e delicado, porém, de acordo com revisão de literatura mostra-se como essencial para o desenvolvimento da segurança cibernética entre os países. Os gestores foram questionados, de forma geral, como eles enxergavam a importância dessa cooperação 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, pode-se observar isso nas afirmações:

> *"Mas eu acho que seria importante os países que são aliados e que têm harmonia, que se cooperem para crescer, porque com compartilhamento os dois lados ganham. Porém acho que assim entre países é mais complicado porque tem a questão da soberania nacional e cada um acha que pode ser invadido."*

> *"Eu acho que existe ainda um mito muito grande aí que se você compartilhar o que você faz de segurança, você pode estar entregando o ouro para o bandido. Então é complicado? Não, não existe muita cooperação não nessa área."*

> *"Tem uma questão muito delicada né? Dentro dos artigos que eu pesquisei, muitos são os países não compartilham as informações. Além de existir a pirataria dos próprios países. Eles vão investigar dados do outro país, então, eles têm interesse nos dados desse outro país"*

> *"Existe essa resistência, principalmente porque o Brasil não escolheu um lado ainda, né? Então, por exemplo, os Estados Unidos não vão querer compartilhar muita coisa com a gente, muita coisa avançada com a gente. Sendo que a gente também coopera com os BRICS nessa área e vice-versa. [...]O Brasil tem essa postura um pouco mais independente e de aproximação na área cibernética com vários países. Mesmo que a gente tenha escolhido dois parceiros principais, a gente não fechou a porta para os outros. E isso pode ser um dos pontos que evita um compartilhamento muito intenso das tecnologias."*

Portanto, os gestores alertam sobre a importância sobre a importância da cooperação entre os países para o desenvolvimento geral, como o compartilhamento de boas práticas. Entretanto existe a delicada questão sobre o compartilhamento de informações que impede a cooperação. Assim sendo, o quadro 9 apresenta os quatro itens que formam o construto "cooperação internacional".

Quadro 9 – Construto Cooperação internacional

CONSTRUTO 9: Cooperação internacional Compartilhamento de boas práticas entre os países para o desenvolvimento da segurança cibernética
47. A OCDE faz um importante trabalho em termos de cooperação internacional. 48. A cooperação internacional é fundamental. 49. A cooperação não é uma prática comum da área. 50. O Brasil possui uma postura independente .

Fonte: Elaborado pelo autor

Segundo Carr (2016), a cooperação internacional é fundamental para o aperfeiçoamento das diretrizes e ações da segurança cibernética. Entretanto, apesar de quase três décadas de esforços diplomáticos, colaboração transversal e atenção acadêmica, a cooperação internacional da segurança cibernética tem sido lenta e incerta. Assim sendo, segundo os gestores a cooperação é essencial para o desenvolvimento da segurança cibernética, principalmente com o compartilhamento de boas práticas. Entretanto, alertam que é fundamental ter cuidado, uma vez que é um tema delicado e o vazamento e pirataria de dados existe. Assim, a soberania nacional sempre deve ser levada em consideração.

5 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

A segurança cibernética é fundamental, hodiernamente, para qualquer organização. São ações e práticas que guiam as organizações com o objetivo de se protegerem de tentativas de ataques cibernéticos. Posto isto, nas organizações públicas a segurança cibernética deve ser vista com fundamental, uma vez que todo o Estado depende do bom funcionamento dos processos tecnológicos e da proteção contra ataques cibernéticos. Observando a dinâmica da segurança cibernética na área pública do Brasil, este trabalho teve como objetivo responder o seguinte questionamento: “Quais são os principais condicionantes da segurança cibernética na administração pública federal brasileira sob a ótica de gestores de TI?”.

Foram realizadas entrevistas semiestruturadas com gestores da área pública que trabalham diretamente com a segurança cibernética, a partir das respostas, o objetivo foi mapear e identificar os principais condicionantes encontrados por esses gestores. Foi possível a identificação de 50 afirmativas que foram agrupadas em 9 construtos que buscaram sintetizar quais os principais condicionantes enfrentados pelos gestores relacionados à segurança cibernética.

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

Um importante resultado que foi identificado é a carência de diretrizes operacionais que os gestores possuem. 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 da área pública que trabalham diretamente com a segurança cibernética, portanto, o estudo realizado apresentou importantes limitações quanto a amostra, o número de entrevistados foi reduzido uma vez que por ser um tema delicado, alguns gestores recusaram a participação o que permitiu considerar apenas os resultados encontrados para os entrevistados considerados**.** Outro ponto de limitação é que as entrevistas são uma representação do discurso pessoal e não necessariamente refletem o comportamento real dos gestores com a organização.

Acredita-se que este trabalho possa contribuir para uma discussão cada vez mais aprofundada sobre a segurança cibernética no Brasil. Uma pesquisa futura com um número maior de participantes seria fundamental para a continuação da discussão. Compreender os condicionantes é elementar para encontrar pontos de superação e desenvolver a segurança cibernética no país. Como citado anteriormente, as pesquisas referentes ao tema no país ainda iniciais e este pode ser objeto para futuras pesquisas com um número maior de participantes, consequentemente, com análises mais robustas. Os construtos identificados podem formar a base de um questionário consolidado a ser aplicado às instituições do governo federal como forma de identificar a evolução e o desenvolvimento da segurança cibernética no país ao longo dos anos.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Diretrizes para segurança cibernética - Requisitos. **ABNT**, 2013

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2007– Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da Informação. **ABNT**, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27032:2015 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. **ABNT**, 2015

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 31000:2009 – Gestão de riscos — Princípios e diretrizes. **ABNT**, 2009.

BALL, M. Cybersecurity investment grows in 2020, but organizations face record data breaches. **Canalys.** Disponível em: https://www.canalys.com/newsroom/cybersecurity-investment-2020. Acesso em: 1 abr. 2022.

BARDIN L. Análise de conteúdo. **Edição revista e ampliada**. São Paulo: Edições 70 Brasil; [1977] 2016.

BECHARA, F. R.; SCHUCH, S. B. Cybersecurity and global regulatory challenges. **Journal of Financial Crime**, 2020.

BECHARA, F. R.; SCHUCH, S. B. Cybersecurity and global regulatory challenges. **Journal of Financial Crime**, v. 28, n. 2, p. 359-374, 2020.

BING, R. S. J. S. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. **Reuters**, 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN. Acesso em: 3 abr. 2022.

BORBÚA, R. V.; CHICANGO, R. P. R.; HERRERA, L. R. Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. **URVIO - Revista Latinoamericana de Estudios de Seguridad**, n. 20, p. 31, 2017.

BRASIL. Decreto n. 10.222, de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União,** Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: Acesso em: 1 abr. 2022.

BRASIL. Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. **Diário Oficial da União,** Brasília, DF**.** Disponível em: http://www.fab.mil.br/portal/defesa/estrategia_defesa_nacional_portugues.pdf. Acesso em: 01 abr. 2022

BRASIL. Decreto n. 8.638, de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. **Diário Oficial da União**. Brasília, DF, 18 de janeiro de 2016a. Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/01/2016&jornal=1&pagina=2&totalArquivos=680. Acesso em: 1 abr. 2022.

BRASIL. Decreto n. 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União.** Brasília, DF, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 1 abr. 2022.

BRASIL. Portaria CDN nº14, de 11 de maio de 2015. Homologa a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018. **Diário Oficial da União.** Brasília, DF, 2015. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf

BRASIL. Decreto n. 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**. Brasília, DF, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 1 abr. 2022.

BRASIL. Lei n. 12.965, de 25 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. **Diário Oficial da União**. Brasília, DF, 2014a. Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=24/04/2014. Acesso em: 1 abr. 2022.

BRASIL. Lei n. 13.709, de 15 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**. Brasília, DF, 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 1 abr. 2022.

BRASIL. Norma Complementar 03/IN01/DSIC/GSIPR. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União**, n. 125**,** Brasília, DF. Acesso em: 1 abr. 2022.

BRASIL. Norma Complementar 04/IN01/DSIC/GSIPR. Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União**, Brasília, DF. n. 156, Acesso em: 1 abr. 2022.

BRASIL. Norma Complementar 05/IN01/DSIC/GSIPR. Criação de Equipes de Tratamento e resposta a Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União,** Brasília, DF. n. 125, Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Acórdão n. 2308/2010 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: **TCU**, 2010e. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/levantamento-de-governanca-de-ti-de-2010.htm. Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Acórdão n. 2308/2010 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: **TCU**, 2010c. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500E3BC0A19993DE040010A8900136B. Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Acórdão n. 2585/2012 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: **TCU**, 2012e. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367. Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Acórdão n. 3117/2014 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: **TCU**, 2014e. Disponível em: http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc. Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Acórdão n. 882/2017 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: **TCU**, 2017. Disponível em: http://portal.tcu.gov.br/imprensa/noticias/nivel-de-governanca-e-gestao-de-tecnologias-da-informacao-e-muito-baixo-1.htm. Acesso em: 1 abr. 2022.

BRASIL. Tribunal de Contas da União. Levantamento Integrado de Governança Organizacional Pública - ciclo 2018. Sumário Executivo. Brasília: **TCU**, 2018. Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-2018/resultados.htm. Acesso em: 1 abr. 2022.

BRASIL. Glossário de Segurança da Informação. **Gabinete de Segurança Institucional**. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em: 1 abr. 2022.

BURGESS, M. **Hackers are targeting hospitals crippled by coronavirus**. Disponível em: https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing?msclkid=a8681d3fb22911ec8abbda4b72ba9965. Acesso em: 2 abr. 2022.

CARR, M. Public-private partnerships in national cyber-security strategies. **International Affairs**, v. 92, n. 1, p. 43–62, 2016.

CASTRO, R. Sites do Ministério da Saúde e ConecteSUS saem do ar após ataque hacker. **OGLOBO**. Disponível em: https://oglobo.globo.com/saude/sites-do-ministerio-da-saude-conectesus-saem-do-ar-apos-ataque-hacker-25313638. Acesso em: 3 abr. 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Incidentes Reportados ao CERT.br. **CERT.br**. -- janeiro a junho de 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/total.html. Acesso em: 02 abr.2022

CENTRO NACIONAL DE CIBERSEGURANÇA. **Quadro Nacional de Referência Para a Cibersegurança**. Portugal, 2019. Disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf. Acesso em: 2 abr. 2022.

CHATTERJEE, D. Should executives go to jail over cybersecurity breaches? **Journal of Organizational Computing and Electronic Commerce**, v. 29, n. 1, p. 1–3, 2019.

CHECK POINT RESEARCH. Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again**. Check Point Software Technologies**. Disponível em: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/. Acesso em: 1 abr. 2022.

CORREIA, P. M. A. R.; SANTOS, S. I. da S.; BILHIM, J. A. de F. Proposta de modelo explicativo das percepções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime. **Sociologia: Revista da Faculdade de Letras da Universidade do Porto**, v. 33, 2017.

COSTA, P. *et al*. The security challenges emerging from the technological developments: A practical case study of organizational awareness to the security risks. **Mobile networks and applications**, v. 24, n. 6, p. 2032–2037, 2019

CYBER EDGE GROUP. **Cyberthreat Defense Report 2021**. Disponível em: https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx. Acesso em: 1 abr. 2022.

DA CRUZ JÚNIOR. S. C. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. Rio de Janeiro: **Instituto de Pesquisa Econômica Aplicada.**, 2013.

DYGNATOWSKI, S.; DYGNATOWSKI, W. Legal basis of cybersecurity on the background of polish and UE legislation. **Journal of KONBiN**, v. 50, n. 4, p. 321–329, 2020.

EUGEN, P.; PETRUT D. Exploring the New Era of Cybersecurity Governance. **Ovidius University Annals: Economic Sciences Series**, p. 358-363, 2018.

EUROPEAN COMISSION. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Disponível em: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667. Acesso em: 02 de abr de 2022.

FÓRUM ECONÔMICO MUNDIAL (FEM). Businesses are building a global response to cybersecurity risks, 2021. Disponível em: https://www.weforum.org/impact/averting-a-cyber-pandemic-businesses-are-building-a-global-response-to-cybersecurity-risks. Acesso em: 26 set. 2018.

GHANN, Patricia; TETTEH, Emmanuel Dortey ; DOE, Nina. The Impact of Covid-19 on Cybersecurity. **International Journal of Recent Contributions from Engineering, Science & IT (iJES)**, v. 10, n. 01, p. 67–75, 2022.

GIL, A. C. Como elaborar projetos de pesquisa. 4ed. **São Paulo: Atlas**, 2009

GÓMEZ, F. S.; PARRA, J. L. Cooperación público-privada en la protección de infraestructuras críticas**. Cuadernos de estratégia**, nº 185, p.171-216, 2017.

GOMEZ, S; PARRA J. L. Cooperación público-privada en la protección de infraestructuras críticas. **Ministerio de Defensa, Secretaría General Técnica**, p. 171–216, 2017.

GONZALES, S. L. de M; PORTELA, L. S. A geopolítica da espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética. **AUSTRAL: Brazilian Journal of Strategy & International Relations**, v. 7, n. 14, 2018

GOUVEIA, J. B. Direito do Ciberespaço e Segurança Cibernética. **Revista Jurídica Portucalense**, p. 59–77, 2021.

GUO, M. China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. **International Journal of Critical Infrastructure Protection**, v. 22, p. 139–149, 2018.

HUANG, T. *et al*. An Online Detection Framework for Cyber Attacks on Automatic Generation Control. **IEEE Transactions on Power Systems**, v. 33, n. 6, p. 6816–6827, 2018.

HUREL, L. M. Cibersegurança no Brasil: uma análise da estratégia nacional. Artigo 54. **Instituto Igarapé**, 2021.

JARMAKIEWICZ, J.; PAROBCZAK, K.; MAŚLANKA, K. Cybersecurity protection for power grid control infrastructures. **International Journal of Critical Infrastructure Protection**, v. 18, p. 20–33, 2017.

JOHNSON, Joseph. **Global Digital Population 2021**. **Statista**. Disponível em: https://www.statista.com/statistics/617136/digital-population-worldwide/. Acesso em: 1 abr. 2022.

JUNIOR, A. F. DE S.; STREIT, R. E. Segurança cibernética: política brasileira e a experiência internacional**. Revista do Serviço Público - RSP**, v. 68, n. 1, p. 107-130, 2017.

KAPONIG, H. Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward. **Connections: The Quarterly Journal**, v. 19, n. 1, p. 21–37, 2020.

KHALILI, J. Coronavirus hospital suspends activity over cyberattack. **Techradar**. Disponível em: https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack. Acesso em: 3 abr. 2022.

KOSTYUK, N. International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic. **Journal of Strategic Security**, v. 7, n. 1, p. 68–82, 2014.

KSHETRI, N. Cybersecurity and Development. **Markets, Globalization & Development Review**, v. 1, n. 2, 2016.

KURE, H.; ISLAM, S. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. **Journal of Universal Computer Science**. p. 1478-1502, 2019.

KURE, H; ISLAM, S. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. **JUCS - Journal of Universal Computer Science**, 2019

LEE, I. Cybersecurity: Risk management framework and investment cost analysis. **Business Horizons**, v. 64, n. 5, 2021.

LOUREIRO, R. Hospital Sírio-Libanês é alvo de ataque hacker nesta segunda-feira**,** 6. **Exame**. Disponível em: https://exame.com/tecnologia/hospital-sirio-libanes-e-alvo-de-ataque-hacker-nesta-segunda-feira-6/. Acesso em: 3 abr. 2022.

MANDARINO JÚNIOR, R.; CANONGIA, C., Livro verde: segurança cibernética no Brasil. Brasília**: Gabinete de Segurança Institucional**, Departamento de Segurança da Informação e Comunicações (GSIPR/SE/DSIC), 2010. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf. Acesso em: 02 de abr de 2022.

MCSHANE, M.; NGUYEN, T. Time-varying effects of cyberattacks on firm value. **The Geneva Papers on Risk and Insurance - Issues and Practice**, v. 45, n. 4, p. 580–615, 2020.

MEDEIROS FILHO, O. O Brasil e a segurança no seu entorno estratégico: América do Sul e Atlântico Sul. **Instituto de Pesquisa Econômica Aplicada**. p. 21–42, 2014

MORESI, E A. D. *et al*. Defesa cibernética: um estudo sobre a proteção da infraestrutura e o software seguro. **In: Conferencia Iberoamericana de Complejidad, Informática y Cibernética**, 2., 2012.

NORRIS, D. F. *et al*. Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. **Public Administration Review**, v. 79, n. 6, p. 895–904, 2019.

OCDE (Organização para Cooperação e Desenvolvimento Econômico). Recommendation on Digital Security Risk Management. **OCDE**, 2015. Disponível em: <https://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf. Acesso em: 2 abr. 2022.

PAIVA, Y. C. Conscientização sobre segurança cibernética na Administração Pública. **Conteudo Juridico**, 2020. Disponível em: https://conteudojuridico.com.br/consulta/artigos/55351/conscientizao-sobre-segurana-ciberntica-na-administrao-pblica. Acesso em: 31 mar 2022

PARK *et al*. The Diagnosis and Prescription for Cybersecurity in Korea: Focusing on Policy and System. **KSII Transactions on Internet and Information Systems**, v. 12, n. 2, 2018.

PONTES, F. STJ é alvo de ataque de hacker e Polícia Federal investiga o sistema. **Agência Brasil.**, 2020. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema. Acesso em: 3 abr. 2022.

PROTRKA, N.; MARIĆ, K.; PLEĆAŠ, M. Challenges and Aspects of Cyber Security of the Republic of Croatia. **Acta Economica Et Turistica**, v. 3, n. 1, p. 87–95, 2017.

RIGUES, R. SolarWinds: ataque foi o "maior e mais sofisticado" já visto. **Olhar Digital**. Disponível em: https://olhardigital.com.br/2021/02/15/noticias/solarwinds-ataque-foi-o-maior-e-mais-sofisticado-que-o-mundo-ja-viu/. Acesso em: 3 abr. 2022.

RODRIGUES, R. Mais de 20% dos PCs ainda usam Windows 7. Disponível em: https://www.kaspersky.com.br/blog/pcs-windows-7-ataques/17550/. Acesso em: 2 abr. 2022.

ROTH, R. J.; DRESSLER, W. Market-oriented conservation governance: The particularities of place. **Geoforum**, v. 43, n. 3, p. 363–366, 2012.

SOOMRO, Z. A.; SHAH, M. H.; AHMED, J. Information security management needs more holistic approach: A literature review. **International Journal of Information Management**, v. 36, n. 2, p. 215–225, 2016.

SOUSA, E. S. DE. A gestão da TI dentro do serviço público. Gestão e Tecnologia para a competitividade, 2013.

SOUZA, E. A. A.; ALMEIDA, N. N. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do estado. **Revista da Escola de Guerra Naval**, v. 22, n. 2, p. 381–410, 2016.

TANCZER, L. M.; BRASS, I.; CARR, M. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. **Global Policy**, v. 9, p. 60–66, 2018.

TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico de gestão de riscos. **TCU**. 2018. Disponível em: https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf. Acesso em: 2 abr. 2022.

TRIVIÑOS, A. N. S. Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação. **São Paulo: Atlas**, 1987. p. 31-79.

UNTERSINGER, M. Le virus Petya a coûté plus d'un milliard d'euros aux entreprises. **Le Monde**, 2017. Disponível em: https://www.lemonde.fr/pixels/article/2017/11/07/le-virus-petya-a-coute-plus-d-un-milliard-d-euros-aux-entreprises_5211421_4408996.html. Acesso em: 31 mar. 2022.

URGESSA, W. G. Multilateral cybersecurity governance: Divergent conceptualizations and its origin. **Computer Law & Security Review**, v. 36, p. 105368, 2020.

VEALE, M.; BROWN, I. Cybersecurity. **Internet Policy Review**, v. 9, n. 4, 2020.

VEIGA, A. et al. Defining organisational information security culture – Perspectives from academia and industry. Computers & Security, p. 101713, 2020.

VIANNA, E. W.; FERNANDES, J. H. C. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos, **Brazilian Journal of Information Science: research trends**, v. 9, n. 1, 2015.

VIEIRA, J. B.; BARRETO, R. T. de S. Governança, gestão de riscos e integridade. **Escola Nacional de Administração Pública**, v. 05, 2019.

WILLETT, M. Cyber instruments and international security. **The International Institute for Strategic Studies**, 2019. Disponível em: https://kclpure.kcl.ac.uk/portal/files/110831207/Conference_Reader_FINAL.pdf#page=10. Acesso em: 31 mar. 2022.

1. APÊNDICES

1. Apêndice 1: Questionário da Entrevista

SEGURANÇA CIBERNÉTICA – GERAL

1. Como você enxerga o panorama atual da Segurança Cibernética no mundo?
2. Você acredita que o Brasil está se desenvolvendo e absorvendo toda a evolução da Segurança cibernética?
3. Na sua opinião, quais são os principais desafios da segurança cibernética na área pública brasileira?
4. Quais seriam as principais ações dos órgãos públicos brasileiros para superar esses desafios?

SEGURANÇA CIBERNÉTICA – ESPECÍFICAS

1. (ESTRUTURA E PROCESSOS) Você acredita que a área pública brasileira possui uma rede adequada, tanto pessoal, como estrutural, relacionada a Segurança Cibernética?
2. (ESTRUTURAS E PROCESSOS) A Estratégia Nacional de Segurança cibernética se mostrou relevante na sua instituição?
3. (ESTRUTURAS E PROCESSOS) A ausência de um órgão central que exerça coordenação executiva da Segurança Cibernética no país, mostra-se relevante?
4. (INFRAESTRUTURAS CRÍTICAS) Quais são as maiores preocupações da organização quanto as ameaças cibernéticas?
5. (GESTÃO DE RISCOS) Existe um planejamento de gestão de riscos cibernéticos?
6. (GOVERNANÇA) Existe uma política ou modelo de governança da segurança cibernética no seu órgão?
7. (LEGISLAÇÃO) Qual o nível de maturidade do arcabouço normativo brasileiro relacionado a Segurança Cibernética?
8. (LEGISLAÇÃO) Em quais aspectos você acredita que a legislação pode prejudicar ou promover o avanço tecnológico do Governo quanto a Segurança Cibernética?

9. (SENSIBILIZAÇÃO E FORMAÇÃO) Quais os principais desafios encontrados relacionados a capacitação e sensibilização em Segurança Cibernética dos gestores encontrados na sua instituição?
10. (SENSIBILIZAÇÃO E FORMAÇÃO) Você acredita que seu órgão fornece a capacitação em Segurança Cibernética adequada?
11. (COOPERAÇÃO INTERNACIONAL) Você enxerga uma cooperação internacional acerca do tema segurança cibernética?