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

SAMARA FERRAZ SCHUENCK

POLÍTICAS PÚBLICAS DE SEGURANÇA DA INFORMAÇÃO NA PREVENÇÃO E TRATAMENTO DE INCIDENTES CIBERNÉTICOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL

Brasília–DF
2022

SAMARA FERRAZ SCHUENCK

POLÍTICAS PÚBLICAS DE SEGURANÇA DA INFORMAÇÃO NA PREVENÇÃO E TRATAMENTO DE INCIDENTES CIBERNÉTICOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL

Monografia apresentada como requisito parcial à obtenção do título de Bacharel em Gestão de Políticas Públicas ao Departamento de Gestão de Políticas Públicas da Universidade de Brasília.

Professora Orientadora: Drª. Christiana Freitas

Brasília–DF

2022

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Ferraz Schuenck, Samara
FS385p POLÍTICAS PÚBLICAS DE SEGURANÇA DA INFORMAÇÃO NA PREVENÇÃO E TRATAMENTO DE INCIDENTES CIBERNÉTICOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL / Samara Ferraz Schuenck; orientador Christiana Soares de Freitas. -- Brasília, 2022.
48 p.

Monografia (Graduação - Gestão de Políticas Públicas) -- Universidade de Brasília, 2022.

1. Segurança da informação. 2. Segurança cibernética. 3. Governo digital. I. Soares de Freitas, Christiana , orient. II. Título.

SAMARA FERRAZ SCHUENCK

POLÍTICAS PÚBLICAS DE SEGURANÇA DA INFORMAÇÃO NA PREVENÇÃO E TRATAMENTO DE INCIDENTES CIBERNÉTICOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Gestão de Políticas Públicas da Universidade de Brasília da aluna Samara Ferraz Schuenck.

_____
Doutora Christiana Soares de Freitas
Professora- Orientadora

_____
Doutor Carlos Marcos Batista
Professor- Examinador

Brasília – DF

2022

Dedico a Jesus, o dono de toda sabedoria e oportunidades de vida concedida a mim, sem ele eu não teria chegado até aqui.

AGRADECIMENTOS

Durante o ensino médio eu sonhava em entrar na Universidade de Brasília (UnB), eu não dormia um dia sequer sem fazer este pedido em minhas orações, e cá estou me formando na UnB rsrs. E neste contexto meu primeiro agradecimento vai a Deus, o dono dos meus sonhos e da minha história. Todas as linhas foram delineadas por ele, desde amigos, professores e minha trajetória profissional.

Destino também, meus sinceros agradecimentos à minha família, mãe e pai: Maristela e Paulo, irmãs: Wanessa e Talita, avô: Hermogenes, tia: Alessandra, amo vocês infinitamente!

Durante todo o período de aprendizagem acadêmica, tive a oportunidade de conhecer pessoas maravilhosas. Dentre elas, estão alguns professores queridos, a primeira foi a Christiana Freitas, a animação e entusiasmo dela em dar aula me fez escolhê-la de primeira como minha orientadora. Outro professor que marcou minha trajetória acadêmica foi o professor Carlos Batista, a paciência e amor pelo o que ele faz é nítido, sempre atencioso com os alunos. Também gostaria de mencionar o professor Franco de Matos, outro professor que é extremamente paciente e ama o que faz. Obrigada meus queridos professores por todos os ensinamentos, saibam que vocês fizeram diferença em minha trajetória acadêmica.

No decorrer de minha vida profissional, fui prestigiada em ser estagiária na Presidência da República, dentro do Departamento de Segurança da Informação (DSI/PR), tive a oportunidade de conhecer pessoas maravilhosas e acolhedoras neste departamento, no qual me deram os maiores apoios possíveis para me tornar uma profissional competente. Obrigada General Oliveira Freitas, Coronel Garcia, Coronel Fontenelle, Major Barreto. Saibam que os Senhores fizeram diferença em minha trajetória profissional.

E por último, não menos importante, muito pelo contrário, está meu namorado Gustavo Marques e sua família. Obrigada meu lindo por todo amor, apoio e carinho conosco durante todas minhas fases boas e de estresse, amo você e sua família.

RESUMO

Fenômeno em constante evolução nos manuseios da Administração Pública Federal (APF), as Tecnologias da Informação e Comunicação (TICs) vem adquirindo importância na rotina de trabalho dos prestadores de serviços para a APF. O trâmite de informações por intermédio do espaço cibernético correspondente às atividades inerentes ao serviço público já é uma realidade. Abordar as políticas públicas destinadas à Segurança da Informação (SI) é um dos caminhos para dispor de uma APF forte, segura e resiliente no que tange aos incidentes cibernéticos. Para isso, buscou-se explorar como o governo federal brasileiro de fato regulamenta essas políticas por meio dos instrumentos de ação pública, tais como Decretos, Instruções Normativas e outros por intermédio do Departamento de Segurança da Informação (DSI), que se localiza na Presidência da República (PR). Os períodos de análise pretendidos desta pesquisa correspondem ao período que vai de 2019 a 2021. Questiona-se como o governo federal brasileiro trata ou busca resolver os incidentes cibernéticos com instrumentos de ação pública na temática de SI. Para isso foi realizado um mapeamento dos instrumentos de ação pública do DSI. Foram analisados os objetivos da Estratégia Nacional de Segurança Cibernética (E-Ciber), além da realização de uma análise de conteúdo a respeito das entrevistas aplicadas aos Gestores especialistas em SI do DSI, relacionando com os objetivos da E-Ciber com o intuito de identificar os desafios nesta estratégia, com base na percepção dos gestores. Conclui-se que os instrumentos de ação pública mais destacados para prevenção e tratamento de incidentes cibernéticos pelos gestores foram a Rede Federal de Gestão de Incidentes Cibernéticos; Estratégia Nacional de Segurança Cibernética (E-Ciber); Política Nacional de Segurança da Informação. Destaca-se que os instrumentos de ação pública no assunto de SI do DSI foram encontrados somente a partir de 2020, representando um avanço a partir deste período a respeito do tema. No entanto, vários desafios em segurança da informação foram encontrados, como encontrar profissionais capacitados na área de segurança cibernética; a conscientização dos cidadãos e a ausência do assunto de segurança cibernética na base comum curricular dos estudantes.

Palavras-chave: Segurança da informação. Segurança cibernética. Governo digital.

ABSTRACT

A relatively constantly evolving phenomenon in the handling of the Federal Public Administration (APF), Information and Communication Technologies (ICTs) has been acquiring significance in the work routine of service providers for the federal public administration, the transmission of information through the cyber space corresponding to the activities inherent to the public service is already a reality, addressing public policies aimed at Information Security (IS) is one of the favorable ways to have a strong, secure and resilient federal public administration with regard to cyber incidents. For this, we sought to explore how the Brazilian federal government actually regulates these policies through public action instruments, such as Decrees, Normative Instructions and others through the Department of Information Security (DSI), which is located in the Presidency of the Republic (PR), the intended analysis periods of this research correspond to the last two years, from 2019 to 2021.It is questioned how the Brazilian federal government treats or seeks to resolve cyber incidents with instruments of public action in the area of Information Security. For this, a mapping of the instruments of public action of the information security department was carried out, in addition, the objectives of the National Cyber Security Strategy (E-Ciber) were addressed, in addition to carrying out a content analysis regarding the interviews applied to managers. information security specialists from the information security department relating it to the objectives of the National Cyber Security Strategy in order to identify advances and challenges in this strategy that are in line with the arguments of the managers interviewed. It is concluded that the most outstanding public action instruments for the prevention and treatment of cyber incidents by managers were the Federal Network of Cyber Incident Management; National Cyber Security Strategy (E-Ciber); National Information Security Policy. In addition, the instruments of public action on the subject of information security of the Department of Information Security were only found from 2020, representing an advance in the last two years, due to having more regulations in these periods. However, regarding the challenges in information security, it is concluded that it is to find trained professionals in the area of cybersecurity; citizen awareness and absence of cybersecurity subject in the common curriculum of students.

Key words: Information security. Cyber security. Digital government

LISTA DE ABREVIATURAS E SIGLAS

AC Análise de Conteúdo

APF Administração Pública Federal

CTIR Gov Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

DSI Departamento de Segurança da Informação

E-Ciber Estratégia Nacional de Segurança Cibernética

ETIR Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

GSI Gabinete de Segurança Institucional

IC Infraestruturas Críticas

IN Instrução Normativa

IoT Internet das coisas

LGPD Lei Geral de Proteção de Dados

MEC Ministério da Educação

PNSI Política Nacional de Segurança da Informação

PR Presidência da República

SEI Sistema Eletrônico de Informações

SI Segurança da Informação

TICs Tecnologias da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO DO TEMA

As Tecnologias da Informação e Comunicação (TICs) possibilitaram avanços no desenvolvimento das atividades na Administração Pública Federal (APF). O governo digital surgiu com o intuito de inovar e aperfeiçoar a própria organização do Estado, com o objetivo de inserir novas tecnologias de forma a acompanhar as evoluções do mundo tecnológico. Com esses avanços significativos, torna-se necessário pensar na Segurança da Informação (SI) no âmbito governamental.

De acordo com Fontes (2006, p. 130), SI é o "conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada". Neste sentido, fica claro que, para um bom desempenho das atividades na APF, é fundamental uma gestão capacitada e vigilante quanto aos incidentes cibernéticos.

Antes de conceituar incidentes cibernéticos, torna-se importante entender os temas interligados que padecem de consequências pela ausência de SI, neste sentido estão as Infraestruturas Críticas (IC). Segundo o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), Decreto n° 9.573 de 22 de novembro de 2018, IC são: "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". Isto significa que a segurança digital das informações das áreas das Infraestruturas Críticas é importante para a manutenção da própria ordem nacional.

Os incidentes cibernéticos estão vinculados aos fatores secundários, ou seja, às aberturas que levam, de fato, ao ataque cibernético. De acordo com a empresa de Soluções em Tecnologia, os incidentes cibernéticos são "a vulnerabilidade ou a fraqueza da infraestrutura de TI de uma organização, que deixam brechas para vários tipos de ataques dos cibercriminosos" (Soluções em Tecnologia - SETI, 2020).

Com os avanços tecnológicos, diversas organizações adotaram como base de suas demandas as ferramentas digitais como caminhos favoráveis para uma gestão mais ágil e eficiente. No âmbito governamental não foi diferente, a APF tem evoluído, o termo "Governo Digital" vem ganhando evidência. Sistemas digitais têm sido adotados pelo governo para facilitar o desempenho dos trabalhos prestados.

De uma sala de arquivos em papel físico, as informações têm sido transportadas para o espaço virtual. De certo modo, anteriormente, a segurança era simplificada pelo fato de estar localizada numa sala de arquivos com chave. Atualmente, é necessário pensar na segurança das informações no ambiente web. Com a transição das informações, a APF ficou mais suscetível aos riscos de roubo de informações, diversos incidentes cibernéticos são notificados no setor público.

Essa pesquisa visa, então, investigar como o governo federal brasileiro age com políticas públicas para Segurança da Informação (SI) em oposição aos incidentes cibernéticos na APF através do Departamento de Segurança da Informação da Presidência da República.

Para esse estudo, a princípio é proposto fazer um levantamento geral dos instrumentos de ação pública, tais como, Decretos, Instruções Normativas, entre outros do Departamento de Segurança da Informação com um recorte nos três últimos anos, de 2019 a 2021. Do mesmo modo, pretende-se abordar os objetivos da Estratégia Nacional de Segurança Cibernética (E-Ciber) do DSI, sendo considerada como um dos instrumentos de ação pública mais relevante do setor (BRASIL, 10.222, 2020). Por fim, foi proposta a realização de entrevistas com alguns gestores deste departamento, além de trazer uma análise de conteúdo de alguns elementos questionados nas entrevistas, nos quais os relaciona com alguns objetivos da E-Ciber. Os elementos ou categorias analisados e discutidos foram: Capacitação; Arcabouço: Dimensão Normativa; Educação em segurança cibernética na base comum curricular.

Esta pesquisa apresenta, também, alguns conceitos fundamentais para compreensão da temática deste estudo, tais como: governo digital; governança digital; segurança da informação; infraestruturas críticas; incidente cibernético; ataque cibernético; espaço cibernético; instrumentos de ação pública.

1.2 PERGUNTA DE PESQUISA

O tema de Segurança da Informação, relativo à prevenção e tratamento de incidentes cibernéticos, vem sendo assunto de discussão nos últimos dois anos para orientação aos Órgãos da Administração Pública Federal por intermédio do Departamento de Segurança da Informação. Para supervisionar questões referentes aos incidentes cibernéticos, algumas medidas/ações são trabalhadas por algumas instituições, dentre elas o Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Segundo a Lei n° 13.844, este Gabinete é o órgão responsável por “coordenar as atividades de segurança da informação e das comunicações no âmbito da administração pública federal” (BRASIL, 13.844, 2019).

Neste Gabinete está o Departamento de Segurança da Informação. Segundo o Decreto n° 10.363, este Departamento é o Órgão responsável por planejar, coordenar e supervisionar as atividades nacionais de segurança da informação, incluindo segurança cibernética, gerenciamento de incidentes de computador, proteção de dados, certificação de segurança e tratamento de informações classificadas. (BRASIL, 10.363, 2020). Os dados desta pesquisa, tais como entrevistas e análises documentais, foram coletados através do Departamento de Segurança da Informação, visando identificar e analisar os instrumentos de ação pública, dentre eles, com um maior destaque para a Estratégia Nacional de Segurança Cibernética.

Com os avanços dos meios digitais, ficou cada vez mais fácil e prático o acesso à informação; a velocidade dessas informações foi ampliada com a implantação das Tecnologias de Informação e Comunicação na APF. No entanto, essas facilidades alargaram as vulnerabilidades e abriram brechas para as informações confidenciais se tornarem invadidas; diariamente, ocorrem ataques cibernéticos que geram consequências, tais como a queda de sites corporativos; instabilidade no sistema da organização; sequestro de dados com possíveis ameaças por parte de hackers; venda de dados, entre outros. Desta forma, o tema de SI tem sido considerado por diversos atores como tema central para uma APF eficaz, segura e resiliente quanto aos incidentes cibernéticos.

Diante desses obstáculos e atores envolvidos nos últimos dois anos, tal como o DSI, com estratégias de segurança, tal como a Estratégia Nacional de Segurança Cibernética, no qual motivou à elaboração da pergunta de pesquisa: como o governo federal buscou resolver os incidentes cibernéticos com instrumentos de ação pública (normas, leis, políticas públicas, programas governamentais, etc) para a segurança da informação no período que vai de julho de 2019 a julho de 2021?

1.3 OBJETIVOS

Objetivo geral

Identificar avanços e desafios no campo do desenvolvimento de instrumentos de ação pública para a Segurança da Informação no governo federal brasileiro.

Objetivos Específicos

Em uma análise aprofundada sobre este tema, foram abordados os seguintes objetivos específicos:

i) Identificar e analisar os instrumentos de ação pública (incluindo os instrumentos normativos, como Leis, Decretos, Instruções Normativas), nos últimos 2 anos (de julho de 2019 a julho de 2021), relacionados à SI do Departamento de Segurança da Informação;

ii) Identificar e analisar alguns objetivos da Estratégia Nacional de Segurança Cibernética (Decreto 10.222, de 5 de fevereiro de 2020);

iii) Identificar e analisar a percepção dos gestores do Departamento de Segurança da Informação sobre o tema, relacionando-a com as ações estratégicas da E-Ciber com intuito de identificar os desafios (no âmbito do DSI) em relação a segurança cibernética[1];

1.4 JUSTIFICATIVA

O Brasil tem caminhado numa articulação cada vez maior com as redes de computadores. No entanto, consequentemente, os incidentes cibernéticos aumentaram de uma forma frenética. Nesta perspectiva, torna-se necessária a segurança cibernética. Silva *et al* (2019) trazem a posição brasileira no que tange à segurança cibernética:

> Identificou-se que o Brasil se encontra em nível intermediário de segurança cibernética, segundo critérios da União Internacional de Telecomunicações. Além de que a maior parte dos ataques cibernéticos sofridos no Brasil reportados ao CERT.br originam-se no próprio país, o que pode ser uma consequência da falta de leis específicas e da sensação de impunidade pelos infratores. (SILVA; NOGUEIRA, 2019, p. 43).

Silva e Nogueira (2019), ao mencionarem que a maioria dos ataques sofridos origina-se no próprio país e justifica esta causa pela ausência de leis específicas no Brasil, traz um dos pontos chaves para a necessidade da pesquisa deste estudo, pois a pretensão é justamente abordar essas regulamentações de forma a verificar como o governo brasileiro tem conduzido e produzido essas legislações.

Um ataque cibernético pode provocar danos irreparáveis, como a perda de dados e prejuízos financeiros. Quando estas perdas estão direcionadas à Administração Pública Federal, transforma-se em uma ameaça ao Estado e à própria ordem nacional.

[1] Área da segurança da informação.

Diante dessas análises, estudos direcionados aos instrumentos de ação pública se tornam fundamentais para compreender os meios utilizados pelo governo para solucionar tais incidentes. Entender como o governo federal institui esses instrumentos se torna importante para compreender as políticas públicas de Segurança da Informação. O entendimento da sociedade na área de governo digital e uma cultura voltada para a SI na APF são meios fundamentais para o segmento de soluções.

No tempo atual, é custoso avistar alguma atividade em progresso por parte da APF e Órgãos que não utilizam as Tecnologias da Informação e Comunicação, já que a maioria dos trabalhos é realizada via internet. Diante disso, torna-se necessário uma atenção a SI no âmbito dessas Instituições.

A SI é um elemento essencial e regularizador para o desempenho da própria organização; sem ela, as redes dos organismos institucionais ficam mais suscetíveis a riscos de invasores com intenções como o roubo de dados operacionais, prejudicando um conjunto de atores, tais como a própria organização, os dados da sociedade que a instituição pode ter acesso, entre outros. Dessa forma, a SI não é apenas uma medida defensiva, mas sim um importante fenômeno para os órgãos conseguirem alcançar seus objetivos de forma segura.

Políticas públicas e legislações de segurança cibernética são imprescindíveis para as infraestruturas críticas, que são direcionadas pela APF e Ministérios, pois trabalham em conjunto para prestar serviços à sociedade, suas áreas de atuação são organizadas por função, tais como, segurança, educação, saúde, água, energia. Todas essas áreas são interligadas. Se um ataque cibernético ocorrer na zona de Usina Hidroelétrica, por exemplo, consequentemente irá prejudicar o setor de energia. Toda a ordenação destas organizações depende das TICs para o gerenciamento de seus afazeres.

O tema da SI na APF é difuso, envolve a gestão, ou seja, a importância do trabalho dos gestores para criar instrumentos normativos destinados à proposta de soluções relevantes, além de também envolver a sociedade. Entender essa complexidade destinada a uma pesquisa dos avanços e desafios é válida. O trabalho do gestor de SI se da pela iniciativa de colocar, na agenda governamental, principalmente dois objetivos: i) identificar as vulnerabilidades cibernéticas; ii) explorar e estudar normas para definir alternativas de solução dentro desta perspectiva.

Para os Órgãos e Ministérios desenvolverem seus trabalhos com excelência para a sociedade, a eficácia e eficiência na gestão de suas atividades através de normas e políticas públicas que regulamentam sua estrutura cibernética são instrumentos fundamentais para

solucionar as vulnerabilidades. Torna-se válido, portanto, um estudo destes instrumentos de ação pública relacionados à APF.

O planejamento, a coordenação e a supervisão da atividade nacional de SI são atividades essenciais para a prevenção e tratamento dos incidentes cibernéticos na APF. Essas competências são do Departamento de Segurança da Informação da Presidência da República (DSI/PR), no qual se dá por criação de legislações específicas com preocupações para distintos atores, tais como uma maior segurança para os Órgãos, para a sociedade e no âmbito do poder Executivo Federal. Essas legislações resultam em uma gestão eficiente, que entrega resultados bons para distintos atores envolvidos.

Legislações voltadas a SI são importantes para o setor financeiro, levando em conta que bancos precisam de políticas de SI, seja para garantir a integridade, confidencialidade e a disponibilidade das informações nos seus sistemas. Além de serem importantes também, quando se trata do setor financeiro, as finanças dos Órgãos e dos Ministérios.

É importante estudar e aprofundar neste tema de SI, levando em conta que também existe certo interesse por parte da sociedade, tendo em vista que os órgãos trabalham em conjunto para a prestação e o desenvolvimento de serviços à comunidade. O armazenamento, coleta, tratamento dos dados dos cidadãos se torna importante; a estrutura e legislações adequadas a um bom funcionamento e tratamento destes dados pessoais é algo imprescindível.

Além da temática de SI ser essencial para vários setores, ela também é primordial para os cidadãos, pois estas organizações lidam com dados pessoais da sociedade, dessa forma a proteção de dados pessoais dos indivíduos é fundamental por intermédio dos instrumentos de ação pública voltados à segurança da informação, pois são os governos que guardam os dados de todos os cidadãos.

2 REFERENCIAL TEÓRICO

2.1 GOVERNO DIGITAL E GOVERNANÇA DIGITAL

Antes de contextualizar e abordar o tema de governo digital torna-se interessante compará-lo com a noção de governança digital. Segundo Renata Crispim:

> Enquanto a Governança Digital engloba aspectos valorativos, subjetivos e políticos, orientados à intensificação da relação entre representantes e representados (via participação cidadã, acesso à inteligência coletiva e outros mecanismos), o Governo Digital possui maior conexão com princípios de administração e economia, que visam resultados, eficiência, efetividade, com destaque para a centralização das ações públicas. (CRISPIM, 2021, p. 32).

Dentro desta perspectiva, o governo digital está focado na atuação estatal, distintos serviços prestados pelo governo à sociedade são acessados por meio do uso da internet. Segundo Heckert e Aguiar, "a literatura destaca o uso das Tecnologias da Informação e Comunicação para aprimorar e automatizar as atividades do governo e suas interações com os diversos segmentos da sociedade, em especial a prestação de serviços" (HECKERT; AGUIAR, 2016, p. 43).

Na transição para o espaço cibernético, no que tange aos serviços prestados pelo governo, a efetividade da Administração Pública Federal tem se mostrado necessária. Os instrumentos utilizados nas interações são por meio dos websites. Neste âmbito, Fountain afirma que os sites podem ser construídos para simplificar o fornecimento de informações e serviços, ou podem ser criados para refletir a organização (descentralizada) e a complexidade das agências governamentais. (FOUNTAIN, 2005).

O governo digital surgiu com o intuito de inovar e aperfeiçoar a própria organização do Estado. Hall e Taylor explicam que, em ambientes incertos e ambíguos, as organizações tentam imitar padrões, sinais e comportamentos que são considerados mais "apropriados" e legítimos para o sistema político. (HALL; TAYLOR, 2003).

O uso de TICs para a atuação governamental, a partir do início da década de 1990, trouxe um aprimoramento na efetividade e eficiência do Estado. Nesta perspectiva, foram criados distintos websites de cunho governamental com objetivos de qualificação na gestão e a prestação de serviços à sociedade; com isso foram reduzidos custos financeiros e operacionais trazendo, de certa forma, eficiência aos manuseios de gestão do Estado.

No entanto, é interessante entender a complexidade enraizada no setor público, qualquer transformação não ocorre ligeiramente. Dessa forma, a dinâmica inovadora de novos

mecanismos implantados na administração do Estado trouxe mudanças nos termos qualitativos e não em modos especificamente voltados para a velocidade. Fountain traz essa concepção direcionada à evolução no serviço público da seguinte forma: "a revolução da informação é uma revolução em termos de significado de seus efeitos não em termos de velocidade" (FOUNTAIN, 2005, p. 151).

As características institucionais em um vínculo com essas técnicas, assim sendo, permitiram um maior conhecimento dos cargos, da estrutura institucional. Nesta concepção, é importante pensar na divulgação de informações, via internet, de organogramas institucionais que a sociedade pode ter o conhecimento sobre a ordenação de determinadas entidades. Kraemer e King reforçam esta ideia, no qual abordam que as tecnologias não afetam a estrutura organizacional do governo. Em vez disso, seu uso visa beneficiar e fortalecer os arranjos institucionais existentes, mantendo o status quo. (KRAEMER; KING, 2006).

Ainda na perspectiva das mudanças, com o uso das TICs para atuação governamental a partir do início da década de 1990, foi possível observar uma complexidade e vários poderes envolvidos, tal como depender da aprovação do legislativo. Qualquer aprovação de lei depende de uma comissão parlamentar, ou seja, envolve um procedimento longo de definições para chegar a uma mudança. A formação desta estrutura burocrática e lenta não se dá apenas pela ausência de mecanismos que atuam de forma a gerar ideias competitivas. Fountain afirma existirem outras questões como, por exemplo, a complexidade das tarefas e processos realizados pelos governos, envolvendo questões de orçamento e propriedade, responsabilidade, jurisdição e distribuição de poder, criando um padrão incremental de mudança. (FOUNTAIN, 2005).

Dentre as peculiaridades das instituições públicas no âmbito digital, é primordial considerar sua distinção com o mercado privado. Fountain (2011) argumenta que as decisões que envolvem a adoção de novas tecnologias e os impactos resultantes diferem nas organizações públicas dos mercados. Os ambientes políticos são muitas vezes caracterizados pela ação coletiva que opera de forma diferente da ação individual. Neles, a natureza do funcionamento das estruturas de autoridade (legislação, normas, regulamentos, etc.) é fundamentalmente diferente das leis que regem as relações de transação de mercado. (FOUNTAIN, 2011).

Com a evolução do uso de recursos digitais na APF, o Governo aderiu ao Sistema Eletrônico de Informações (SEI), que possui o seguinte objetivo:

> com a finalidade de dar agilidade aos processos e documentos, mais transparência e principalmente na redução de custos, permitindo um sistema que arquivasse, produzisse, tramitasse, avaliasse, usasse e guardasse permanentemente documentos

> ou os eliminasse, tudo de acordo com o Conselho Nacional de Arquivos (CONARQ), ambos trabalharão no intuito de aparelhar o Processo Eletrônico Nacional (PEN), apresentando como características principais a portabilidade e o acesso remoto através de todos os navegadores e aparelhos eletrônicos conectados à rede mundial de computadores (internet). (ALBUQUERQUE *et al*, 2017, p. 349).

O SEI surgiu a partir de uma concepção de evolução e modernização dos recursos de trabalho. O Estado precisa buscar novas respostas e soluções em relação a uma administração necessitada de criatividade, conhecimento e inovação.

A praticidade e melhoria que o SEI trouxe para a APF resultou em vários benefícios. Segundo Fernando Aguiar,

> Trata-se de uma grande revolução na administração pública federal e os benefícios são enormes. Pode-se citar economia de recursos com papel, tinta, pastas, maior celeridade na tramitação de processos, padronização dos documentos, mapeamento de processos, maior segurança e redução de espaço físico quanto ao armazenamento dos mesmos, além de proporcionar mais transparência, já que todos os servidores poderão ter acesso a todos os documentos tramitados dentro da instituição, com exceção dos restritos e sigilosos que são estabelecidos por lei. (AGUIAR, 2018, p. 6).

Dessa forma, percebe-se uma grande evolução com o surgimento do SEI, a facilidade que ele trouxe para a APF é bem nítida, tal como uma melhora no recurso de tempo e nas atividades desempenhadas no trabalho, entre outros.

Já na relação com os cidadãos, foi possível observar sua maior participação nas políticas públicas, pois a estrutura governamental digital possibilitaria o acesso a informações e o indivíduo de agente passivo se tornaria participativo na construção das políticas públicas. Dessa forma, o Estado não é o único a tomar decisões e iniciativas no âmbito dessas políticas. Nesta perspectiva, Aguiar aborda que "a utilização de ferramentas eletrônicas como estratégia de Governança Digital para o desenvolvimento de uma gestão pública mais eficiente, moderna, desburocratizada e participativa, já é uma realidade no âmbito da Administração Pública Brasileira." (AGUIAR *et al*, 2018, p. 1).

Segundo Gartner (2000), essa governança digital transforma as relações internas e externas do Estado por meio da tecnologia, da Internet e das novas mídias, permitindo a otimização contínua da prestação de serviços, engajamento dos cidadãos e governança. (GARTNER GROUP, 2000).

2.2 SEGURANÇA DA INFORMAÇÃO

Nos últimos anos, as comunicações têm sido mais ágeis e rápidas, levando em conta que o mundo está digital. Com as organizações não tem sido diferente. Os indivíduos conseguem ter acesso a decretos, leis e normas que regem estruturas organizacionais e relações institucionais de forma mais rápida por meio da internet. A interação da sociedade com os meios digitais faz com que os indivíduos também fiquem suscetíveis aos riscos.

A conexão da sociedade, setores público e privado permite o compartilhamento de informações de uma forma rápida e em tempo real. Com as evoluções dos sistemas de gestão na Administração Pública Federal, torna-se necessário pensar na Segurança da Informação no âmbito administrativo. Com o advento e evolução das Tecnologias da Informação e Comunicação, iniciou-se uma maior amplitude e alcance das informações. Segundo Sêmola:

> Os antigos, mas sobreviventes mainframes não cumpriam mais sozinhos a tarefa de armazenar e processar as informações. Os computadores tomavam conta dos ambientes de escritório, quebravam o paradigma de acesso local à informação e chegavam a qualquer lugar do mundo através da rede mundial de computadores: a Internet. (SÊMOLA, 2014, p. 25).

Através dos computadores, as informações são espalhadas com rapidez; com o passar do tempo, essas capacidades têm se estendido mais ainda, levando em conta que a sociedade da informação possui comodidades de aparelhos de altas tecnologias e que são fáceis de transportar. Com todas essas evoluções, consequentemente, aumentam também os riscos. As facilidades que as tecnologias trouxeram para a sociedade em termos de deslocamento e tempo promoveram as vulnerabilidades. A informação é um elemento poderoso que gera impactos na sociedade e nas organizações.

Fontes conceitua que a informação é muito mais do que um conjunto de dados. Transformar esses dados em informação é fazer sentido de informações avulsas e transformá-las em um recurso valioso para nossa vida pessoal ou profissional (FONTES, 2006).

Para a proteção das informações em qualquer ambiente ou organização, torna-se necessária certa responsabilidade por parte do agente possuidor de tais informações. Essas responsabilidades são regulamentadas por políticas e regras. A informação é um meio crucial para o desempenho das atividades na organização.

Segundo Fontes, as regulamentações de segurança da informação (políticas, normas e regras) são elaboradas para tornar o uso das informações em uma organização mais

organizada para que os negócios não sejam prejudicados pelo uso indevido das informações, seja por engano ou acidente (FONTES, 2006).

Para a realização das demandas nas organizações são necessários meios e recursos para inserir as informações, ou seja, existe uma dependência por parte dos funcionários e servidores públicos às ferramentas de trabalho. A proteção dos meios de comunicação se torna crucial para a imagem da organização. Devido a essa dependência, de certa forma, a instituição está mais suscetível às vulnerabilidades.

Fontes menciona que a segurança da informação existe para minimizar os riscos de negócios associados ao uso de recursos de informação para permitir que uma organização funcione. Sem informações ou a partir de informações incorretas, uma empresa pode sofrer perdas que comprometem suas operações e o retorno do investimento de seus acionistas (FONTES, 2006).

Oliveira, Gomes, Lopes e Nobre também conceituam a Segurança da Informação, "relacionado à proteção de um grupo de informações que busca preservar o valor que estas possuem para uma pessoa ou organização" (OLIVEIRA; GOMES; LOPES; NOBRE, 2019).

Atualmente, existem diversos dispositivos tecnológicos que atuam no desempenho das atividades da sociedade e até mesmo nos trabalhos organizacionais. Estes meios tecnológicos, muitas vezes, são extremamente pequenos, o aperfeiçoamento tem mostrado que praticamente a tecnologia está indo por caminhos sem limites. Porém, nos dias de hoje, a existência de legislações regulamentam e estabelecem limites dos graus de avanços digitais com vistas a SI.

Na perspectiva da proteção do cidadão, uma lei bem atual é a Lei Geral de Proteção de Dados (LGPD), no qual estabelece ordens quanto ao tratamento dos dados de alguns indivíduos por parte das empresas e corporações. Desta forma, deve ser dada uma respectiva atenção ao tema de SI nas organizações que manuseiam informações da sociedade. Segundo o artigo Segurança da Informação para internet das coisas (IoT), onde a "SI é negligenciada, cria-se um desafio para a existência e continuidade do mesmo, pois a SI envolve diversos campos da tecnologia e documentação, assim como possui estrita ligação com setores jurídicos e de RH das organizações." (OLIVEIRA *et al*, 2019, p. 4)

Para a proteção dos dados dos cidadãos é relevante uma gestão equipada suficientemente. Ao encontro desta ideia, é importante pensar nas estruturas das organizações. A APF possui documentos de arquivos sigilosos; logo, pensar na SI, na capacitação da gestão para lidar com o sistema é essencial para uma administração segura.

Sem segurança, uma organização dificilmente sobreviverá. As tecnologias possibilitaram a transmissão de informações sem utilizar documentos de arquivos físicos,

transportes para levar informações, papel, entre outros. Anteriormente, a complexidade dessas transmissões de conteúdos envolvia um maior tempo comparado com as informações transmitidas pelas tecnologias.

Anteriormente, as organizações eram compostas por documentos de arquivo físico, ou seja, poderiam inseri-los numa sala e trancar. A SI, de certo modo, era menos complicada. Com o advento das tecnologias de informação e comunicação, surgem mais necessidades de segurança aos suportes, que antes eram postas numa caixa e foram transportadas para o ambiente virtual; no entanto, de uma forma mais complexa, surgem às ideias de pensar na segurança do ambiente virtual.

De acordo com Fontes (2006), "a informação, independente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos".

Para qualquer organização, a informação é um elemento valioso, visto que sem elas provavelmente não teria como dar continuidade às demandas do trabalho. Desta forma, pensar na segurança do suporte da informação é um dos passos iniciais. Respectivamente, para o desempenho e sucesso da segurança da informação em qualquer organização, são essenciais seus três princípios básicos: o da Confidencialidade, Integridade e Disponibilidade. Fernandes aponta que:

> Conforme descrição feita pela norma ISO/IEC 17799, a proteção da informação é vital, sendo caracterizada pela trilogia CID, ou seja, Confidencialidade, Integridade e Disponibilidade. (INFORMA BR).
>
> Confidencialidade: Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização. (FERNANDES, 2013, p. 84).
>
> Integridade: Garante que a exatidão e completeza das informações não sejam alteradas ou violadas. Um exemplo, vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento!!! (FERNANDES, 2013, p. 85).
>
> Disponibilidade: Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando! (FERNANDES, 2013, p. 84).

Dentre esses princípios, na abordagem da confidencialidade, somente pessoas autorizadas podem acessar as informações. Para o êxito, torna-se interessante pensar na estrutura de gestão em relação aos controles de acessos, ou seja, uma atenção deve ser direcionada à validação por sistemas de senhas. O da Integridade diz respeito à clareza das informações; no entanto, é importante prezar pela segurança dos sistemas de websites

corporativos para não serem corrompidas e alteradas suas informações. Já o da disponibilidade está ligado ao perfeito funcionamento da rede, ou seja, a eficácia do sistema deve ser objeto de importância dentro das organizações.

2.3 INFRAESTRUTURAS CRÍTICAS

Com os avanços tecnológicos e a Era Digital na APF, os riscos e vulnerabilidades surgiram na gestão das organizações do Estado, seja para roubar informações ou prejudicar os serviços básicos prestados à sociedade. As consequências dessas vulnerabilidades podem afetar as Infraestrutura Críticas (IC). Segundo o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), Decreto n° 9.573 de 22 de novembro de 2018, IC são: "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, 2018).

Com os avanços no Setor público foi possível a utilização de sistemas informatizados no desempenho de suas atividades, tais como no âmbito estratégico de uma coletividade na esfera das IC, como transportes, energias, abastecimento de água, saúde, entre outras.

Esses campos básicos, de extrema relevância, garantem a sobrevivência da sociedade. Quando atingidos, podem gerar grandes impactos, inclusive relacionados à segurança nacional. As Infraestruturas Críticas são importantes para o desenvolvimento do país, até mesmo pelas suas facilidades e utilidades que fornecem à sociedade.

Segundo o (CDN/SE, 2009) e (CANONGIA *et al* 2010):

> As *Infraestruturas Críticas da Informação* (ICI) são definidas como o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (CDN/SE, 2009).

Nesta perspectiva, estes meios de armazenamento, no qual é mencionado acima, estão guardadas as informações importantes de manutenção das estruturas básicas de serviços prestados à sociedade, no qual deve ser dada uma atenção especial de segurança, pois se um ativo das áreas desses serviços essenciais forem atingidos, toda a cadeia pode também ser comprometida. Como exemplo está à interdependência da água e energia. Logo adiante é mais aprofundado a respeito desta interdependência:

> As *Infraestruturas Críticas de Informação* possuem a peculiar característica de poderem fazer parte, com relações de interdependências horizontais, de várias Infraestruturas Críticas, ou seja, a informação gerada por determinada área prioritária das Infraestruturas Críticas pode ser insumo para outra, evidenciando, desta forma, o alto grau de acoplamento e interdependência existente entre elas. (CANONGIA *et al*, 2010, p. 28).

Nesta perspectiva da interdependência, podemos dar como exemplo as Usinas Hidroelétricas. Se sofrerem algum determinado ataque cibernético, consequentemente, o setor de energia também será atingido. Segundo Canongia, "tal fato eleva a necessidade da identificação dos ativos de informação essenciais, bem como o tratamento dos riscos a que estes ativos estão expostos, pois o impacto causado pela perda ou indisponibilidade destes ativos pode comprometer toda a cadeia de Infraestruturas Críticas existentes." (CANONGIA *et al*, 2010, p. 28).

Diante dessas perspectivas, observa-se a necessidade de uma APF resiliente e eficaz ao lidar com invasões aos sistemas organizacionais, no âmbito de manter a integridade e desenvolvimento nacional. Além de ser importante para a sociedade, que depende das atividades de água, energia, transporte e outras.

2.4 ESPAÇO CIBERNÉTICO

Com o avanço da informação, através dos meios digitais, o espaço cibernético se tornou evidente. Oliveira *et al*, define o espaço cibernético no qual consiste em dispositivos de computação, com ou sem rede, que transmitem ou armazenam informações. (OLIVEIRA *et al*- 2017). Klimburg estabelece que "o espaço cibernético é mais que internet, inclui não somente hardware, software e sistemas informacionais, mas também pessoas e suas interações sociais nas redes de computadores". (KLIMBURG, 2012, p. 8).

Desta forma, o espaço cibernético é complexo e extensivo, nestes dois conceitos envolve duas concepções, tal como a sua semelhança com a internet e a composição deste espaço cibernético. No primeiro conceito traz a ideia de um espaço cibernético definido como objeto distinto da internet, ou seja, sua extensão é mais prolongada que a web. No segundo conceito, traz a representação de sujeitos nas relações interativas deste espaço.

Simultaneamente, o conjunto de abrangência que envolve este espaço cibernético, apresenta relações interdependentes para sua existência, sem as organizações e órgãos que estruturam os sites profissionais, por exemplo, dificilmente iriam existir os websites- um espaço cibernético para a sociedade interagir e solucionar suas necessidades. Sem os

indivíduos e seus manuseios, este espaço cibernético também não existiria, ou seja, existe uma troca de distintos atores na interação social com o ambiente web. A APF precisa deste espaço para gerenciar suas atividades; a sociedade depende de alguns mecanismos de extensão dos websites, tais como cadastros, acesso às informações de relevância, inscrições, aplicativo de bancos, etc.

2.5 INCIDENTES E ATAQUES CIBERNÉTICOS

De acordo com a SETI, os incidentes cibernéticos são “a vulnerabilidade ou a fraqueza da infraestrutura de TI de uma organização, que deixam brechas para vários tipos de ataques dos cibercriminosos” (SETI, 2020).

É perceptível, então, que os incidentes estão mais relacionados com a estrutura, prevenção, riscos e a percepção das vulnerabilidades para prevenir o acidente, ou seja, o ataque cibernético.

Já o termo acidente se refere ao ataque cibernético, que pode ocasionar perda de dados, roubo de senhas e prejuízos financeiros em decorrência destes ataques. Em relação à definição de ataque cibernético, de uma forma mais genérica, de acordo com Silva e Nogueira, “se trata de uma tentativa maliciosa premeditada de ataque para quebrar a confidencialidade, integridade ou disponibilidade de informações existentes em computadores ou redes computacionais” (SILVA; NOGUEIRA, 2019, p. 44).

Quando se fala em ataque cibernético, é interessante pensar nos atores responsáveis por esses ataques, são designados como hackers. Segundo Ramalho, hacker é definido como alguém com excelentes conhecimentos de informática (RAMALHO, 2002).

A compreensão dos distintos tipos de ataques se torna fundamental para chegar ao desenvolvimento de resoluções e tratamento a cada tipo específico de ataque. De acordo com Washington, “os ataques cibernéticos podem ocorrer de diversas outras formas, como Cavalos de Tróia, backdoors, botnets, spywares, phishing, spear phishing, entre outros” (SILVA; NOGUEIRA, 2019, p. 45).

2.6 INSTRUMENTOS DE AÇÃO PÚBLICA

Segundo Lascoumes e Le Galès, compreende-se instrumento de ação pública como “o conjunto dos problemas colocados pela escolha e o uso dos instrumentos (técnicas, meios de

operar, dispositivos) que permitem materializar e operacionalizar a ação governamental". (LASCOUMES; LE GALÈS, 2012, p.20). Ainda segundo os autores,

> A sociologia do Estado e do governo se interessa há longo tempo pela questão das tecnologias de governo, entre estes os instrumentos da ação pública. A título indicativo é possível catalogar minimamente esses instrumentos: legislativo e regulador, econômico e fiscal, convenção e incentivo, informativo e de comunicação. (LASCOUMES; LE GALÈS, 2012, p. 20)

Os instrumentos de ação pública podem atuar com objetivos mais profundos, ou seja, evidenciar as proporções, que até então não eram tão evidentes, como as competências de dominação. Os instrumentos de ação pública fazem uma análise interpretativa do social e são emissários de valor. Sendo assim, um instrumento de ação pública constitui um dispositivo ao mesmo tempo técnico e social que organiza relações sociais específicas entre o poder público e seus destinatários em função das representações e das significações das quais é portador. (LASCOUMES; LE GALÈS, 2012, p. 21)

Pensar nos instrumentos de ação pública se baseia na ideia de como as instituições estruturam suas políticas públicas. Fundamental também é o conceito de instrumentos de ação pública. Pierre Lascoumes e Patrick Le Galès os definem como “um dispositivo técnico com vocação genérica portador de uma concepção concreta da relação política/sociedade e sustentado por uma concepção da regulação.” (LASCOUMES; LE GALÈS, 2012, p. 22).

Nesta perspectiva, é fundamental articular os instrumentos técnicos como portadores de regulação para ter uma APF resiliente em termos dos incidentes cibernéticos. A importância desses instrumentos de ação pública se reflete na obtenção da autoridade de regulação do mesmo.

Os instrumentos são instituições, técnicas e meios, como instruções normativas, decretos e leis que atuam no âmbito de estruturar a APF em relação aos incidentes cibernéticos. A ferramenta é uma pequena parte dentro da técnica, como exemplo, a especificação de uma responsabilidade posto num determinado texto.

Nas interações relativas de qualquer organização, para seu respectivo desenvolvimento e crescimento, é fundamental as ordens e papéis definidos a cada ator. Nesta concepção, por exemplo, está a responsabilidade individual de cada integrante da organização em manter a segurança das informações da instituição. North traz essa ideia, afirmando que uma instituição consiste em um agrupamento mais ou menos coordenado de regimentos e procedimentos que regem as interações e o comportamento de atores e organizações. (NORTH, 1990). Essas medidas são essenciais para a eficácia das atividades; por meio delas, a imagem da instituição não fica distorcida e passa credibilidade através da organização da interação das áreas dentro

de cada setor. Lascoumes e Le Galès reforçam esta ideia ao afirmar que “as instituições fornecem, assim, um quadro estável de antecipações que reduz as incertezas e estrutura a ação coletiva.” (LASCOUMES; LE GALÈS, 2012, pg 23).

Segundo March e Olsen, na interpretação sociológica resistente, ou a mais a pequena distância do culturalismo, entende-se que essas normas de conduta, tais como os comportamentos adequados, são adquiridas por matrizes cognitivas e normativas, classes coordenadas de princípios, de crenças e de convicções de ação, como a ética. (MARCH; OLSEN, 1989).

Tais instrumentos, como instituições, definem o comportamento dos atores de uma forma previsível quanto aos acontecimentos futuros. Os instrumentos basicamente ditam as regras de interação do ambiente organizacional, ou seja, quais os meios podem ser explorados e por quem estes meios podem ser usados. Desta forma, traz uma facilidade no âmbito da antevisão quanto às ações dos atores.

3 MÉTODOS E TÉCNICAS DE PESQUISA

3.1 METODOLOGIA

A metodologia adotada nesta pesquisa destinou-se a uma análise dos instrumentos de ação pública, tais como Decretos, Instruções Normativas, Leis que integram as estratégias governamentais do Departamento de Segurança da Informação (DSI) da Presidência da República, todos dedicados ao tema da segurança da informação. A construção deste trabalho também foi realizada mediante pesquisa bibliográfica, com o suporte literário de artigos, livros e monografias remetidos aos temas de governo digital, segurança da informação, incidentes cibernéticos, espaço cibernético, instrumentos de ação pública. A oportunidade de participar do DSI despertou curiosidades e facilidades no interesse de investigar o tema da segurança da informação.

Para a construção de um trabalho de pesquisa de excelência, a metodologia é extremamente importante. A metodologia consiste em explicitar os caminhos adotados para chegar a compreensões, reflexões ou resultados. Os caminhos e procedimentos adotados possuem finalidades. Segundo Minayo (1992), essas finalidades possibilitam instituir uma interpretação das informações adquiridas, no qual comprova ou não as conjecturas da pesquisa ou atende às interrogações elaboradas, além de estender o conhecimento no que diz respeito à temática pesquisada, relacionando-a com a situação cultural da qual faz parte.

O estímulo da elaboração desta pesquisa, por ter sido aflorada pelo ato de desvelo e de interesse no assunto, possui uma modalidade exploratória. Laville e Dionne (1999) caracterizam o modelo aberto dentro da perspectiva exploratória, no qual ele traz a seguinte definição:

> O Modelo Aberto: o recurso a uma grade aberta é frequente nos estudos de caráter exploratório, quando o pesquisador conhece pouco a área em estudo e sente necessidade de aperfeiçoar seu conhecimento de uma situação ou de um fenômeno a fim de enunciar hipóteses. (LAVILLE; DIONNE, 1999, p. 219)

Segundo as autoras, nesse modelo aberto, "as categorias não são fixas no início, mas tomam forma no curso da própria análise." (Laville; Dionne, 1999, p. 219). Nesta perspectiva está a modalidade exploratória, que se destina à compreensão do assunto através de consultas e pesquisas. Para a coleta de algumas informações relacionadas à segurança da informação foram realizadas entrevistas com alguns Gestores do DSI/PR. O intuito destas entrevistas

destinou-se à análise da percepção desses atores a respeito das formas de regulação já instituídas - mediante a construção de instrumentos de ação pública - e à compreensão dos desafios relacionados à Segurança da Informação no DSI de 2019 a 2021.

A exploração das fontes leva a caminhos de conhecimento. Esta pesquisa trabalhou com o método indutivo. De acordo com Laville e Dionne, o método indutivo "permite antes construir novos conhecimentos, chegando, por dedução, à ampliação desses conhecimentos." (Laville; Dionne, 1999, p. 22). Ou seja, este método direciona para caminhos argumentativos baseados nas interpretações e concepções do assunto explorado.

Foi trabalhada a triangulação de métodos, com pesquisa documental, levantamento bibliográfico e as entrevistas, que foram designadas a uma coleta de informações de forma qualitativa. De acordo com Bauer, "a pesquisa qualitativa lida com interpretações das realidades sociais e é considerada pesquisa *soft*. 0 protótipo mais conhecido é, provavelmente, a entrevista em profundidade." (BAUER, 2017, p. 23). Nesta concepção, as entrevistas tiveram o intuito de aprofundar a aplicabilidade das Políticas Públicas com vistas à segurança da informação no dia a dia dos Gestores que lidam com a temática em seu ambiente de trabalho.

Este trabalho foi um estudo de caso, por considerar as ações resolutivas do Órgão DSI, fazer uma análise do mesmo e estudar o fenômeno com certa profundidade, é uma das características do estudo de caso. Nesta perspectiva, Laville e Dionne afirmam que o "estudo de caso visa sobretudo à profundidade" (Laville; Dionne, 1999, p. 157). O estudo de caso destinado a esta pesquisa também, além da descrição, visou uma análise interpretativa.

Quadro 1 — Metodologia

TIPO DA PESQUISA	Pesquisa exploratória
TRATAMENTO DOS RESULTADOS	Qualitativo
MÉTODO UTILIZADO	Indutivo
MÉTODO DE PROCEDIMENTO	Estudo de caso em SI no DSI
MÉTODO DE ABORDAGEM/ INSTRUMENTO DE COLETA DE DADOS	Pesquisa documental para identificação e análise dos IAP/ Entrevistas aplicadas aos gestores de Segurança da Informação do Departamento de Segurança da Informação (DSI).

Fonte: autoria própria.

O período analisado nesta pesquisa foi de julho de 2019 a julho de 2021. O tema da segurança da informação ganhou destaque nos ramos governamentais nestes períodos e,

também, aconteceu um evento relevante no organograma da Presidência da república referente ao Departamento de Segurança da Informação. Anteriormente, o Departamento era subordinado à Secretaria de Coordenação de Sistemas, de acordo com o antigo e revogado Decreto n° 9.668, de 2 de janeiro de 2019 (BRASIL, 2019a). Porém, a importância dos assuntos tratados por este Departamento levou sua promoção ao mesmo nível da Secretaria de acordo com o Decreto n° 10.363 de 21 de maio de 2020 (BRASIL, 2020c).

No que se refere às atividades do Departamento de Segurança da Informação, de acordo com o Decreto nº 10.363, ao departamento "compete, planejar, coordenar e supervisionar a atividade nacional de segurança da informação, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas" (BRASIL, 2020c).

3.2 PESQUISA DOCUMENTAL

De acordo com Lima, "a documentação é fundamental no processo de obtenção e análise de dados" (LIMA *et al*, 2007, p. 93). Nesta perspectiva, a pesquisa documental trata-se da pesquisa em documentos, políticas, ações, leis, entre outros. Por este ângulo, esta pesquisa, na concepção da análise das legislações, de certa forma já dispõe de um perfil documentado, visando uma análise descritiva dos documentos oficiais que são instrumentos do governo federal que atuam na segurança da informação para regularizar e solucionar os incidentes cibernéticos.

A delimitação da escolha do Órgão Departamento de Segurança da Informação e seus instrumentos de ação pública se deram pelas experiências, observações e as realizações destes instrumentos que são as Instruções Normativas, Decretos, entre outros. Todos elaborados pelo DSI, com objetivos de proporcionar a segurança da informação em âmbito nacional. A análise destes documentos foi de caráter descritivo numa concepção indutiva. Segundo Angrosino, a análise descritiva é "o processo de tomar o fluxo de dados e decompô-lo em suas partes constitutivas; em outras palavras, que padrões, regularidades ou temas emergem dos dados?". (ANGROSINO, 2009, p. 90)

Quanto à fonte destes documentos, por ter um caráter oficial e regularizador, procedem de fontes secundárias. O acesso a eles está localizado no site do planalto, Presidência da República, a estrutura e descrição destes instrumentos regulamentares, geralmente estão consignados via web, inicialmente: www.planalto.gov.br/ccivil_03/ (...). A

análise e descrição destes instrumentos foram de natureza qualitativa, no qual foram abordados os objetivos e estratégias de cada instrumento de ação pública.

3.3 ENTREVISTA

Segundo Angrosino, “entrevistar é um processo que consiste em dirigir a conversação de forma a colher informações relevantes.” (ANGROSINO, 2009, p. 61). Nesta perspectiva, a pesquisa foi aplicada em formato de entrevista a alguns integrantes do Departamento de Segurança da Informação (DSI), que se localiza no Palácio do Planalto, Presidência da República, em Brasília-DF.

A entrevista, no entanto, tem o papel de investigar os assuntos amplamente discutidos em um grupo focado no assunto que entende da temática neste estudo. Nesta perspectiva, Angrosino menciona que “é necessário, então, começar a fazer perguntas às pessoas bem informadas na comunidade ou no grupo em estudo” (ANGROSINO, 2009, p. 61). Neste sentido, a especialização sobre o tema é fundamental para a coleta de informações. Logo, as perguntas de caráter exploratório foram aplicadas a um conjunto de especialistas no assunto de segurança da informação que lidam e vivenciam na prática esta temática.

A delimitação e escolha do grupo se deram em virtude de suas experiências sobre o assunto em segurança da informação e por constituir-se no ramo do DSI. As entrevistas foram manuseadas de forma presencial, em formato de gravação/ vídeo/ áudio. Segundo Angrosino, gravação é o “modo de assegurar a exatidão do que é dito e, no caso de histórias orais/ de vida, é essencial ter a fala verdadeira pronta para ser ouvida novamente” (ANGROSINO, 2009, p. 68).

O propósito das entrevistas foi ter um roteiro previamente definido e aberto a novas ideias, concepções e perguntas. Por ser um tema difuso e com objetivos exploratórios as entrevistas foram semiestruturadas. De acordo com Angrosino, “A entrevista semiestruturada segue de perto o tópico escolhido de antemão e apresenta questões destinadas a extrair informação específica sobre aquele tópico.” (ANGROSINO, 2009, p. 67). Diante disso, a princípio, foram aplicadas cinco questões, todas iguais para os seis entrevistados, com objetivos de extrair conhecimentos sobre a temática e atuação do DSI, além de obter informações dos objetivos desta pesquisa acadêmica.

A elaboração do roteiro de entrevista deu-se por uma observação ao referencial teórico, ou seja, baseado numa análise de conteúdo, além das perguntas contidas nela serem homogêneas para os respectivos participantes. Segurança da informação é um assunto

genérico, dessa forma, foi realizado um recorte de forma a colher informações e conceitos relacionados à atuação do DSI.

3.4 ANÁLISE DE DADOS

Após a realização da coleta dos dados foram analisados os decretos, instruções normativas e as entrevistas, no qual foi necessária a análise dos resultados. O tratamento dos dados coletados nesta pesquisa será mediante Análise de Conteúdo (AC), que possui algumas etapas fundamentais.

3.4.1 Análise de conteúdo

De acordo com Laurence Bardin, Análise de Conteúdo é um conjunto de técnicas de análise da comunicação que visa obter uma descrição sistemática e objetiva do conteúdo da informação por meio de procedimentos, indicadores (quantitativos ou não quantitativos), permitindo inferir conhecimentos relacionados às condições de produção/recepção dessas mensagens. (BARDIN, 1977).

Nesta perspectiva, o método de descrição da entrevista é fundamental para compreensão dos resultados. Esta pesquisa foi analisada minuciosamente pela técnica AC. Segundo Bardin, a técnica de AC consiste em três etapas principais: 1) pré-análise, 2) exploração dos materiais, 3) processamento e interpretação dos resultados. (BARDIN, 1977). Basicamente, esses três passos são cruciais para um bom desempenho e demonstração de resultados científicos.

De acordo com Bardin, a primeira etapa consiste na etapa de estágio organizacional, durante a fase de organização, diversos procedimentos podem ser utilizados, tais como: skimming, premissas, metas e elaboração de indicadores para subsidiar a interpretação. (BARDIN, 1977). Nesta perspectiva, a entrevista vai consistir numa análise literária, com organização, transcrição e levantamento das informações. Serão direcionadas observações explicativas e resumos das ideias principais das entrevistas, corrigindo eventuais repetições de fala.

Nesta primeira etapa, no desenvolvimento da pesquisa foram abordadas algumas hipóteses de acordo com o objetivo do projeto. A escolha dos itens vai se basear nos

argumentos levantados durante as entrevistas que coincidem com a Estratégia Nacional de Segurança Cibernética[2]

Conforme essas etapas mencionadas por Bardin, Caregnato faz considerações, “na segunda etapa os dados são codificados a partir das unidades de registro.” (CAREGNATO *et al*, 2006, p. 683). Nesta fase foi realizado um delineamento de unidade de registro, o objetivo nesta etapa da pesquisa consistiu em codificar os termos temáticos, como exemplo o item “capacitação”.

Segundo Caregnato, “Na última etapa se faz a categorização, que consiste na classificação dos elementos segundo suas semelhanças e por diferenciação, com posterior reagrupamento, em função de características comuns.” (CAREGNATO *et al*, 2006, p. 683). Por este ângulo, neste projeto foi realizado um levantamento dos termos abordados nas entrevistas que coincidem com a E-Ciber.

Será realizado um recorte categorial dos termos/ palavras semelhantes pelos seis entrevistados para uma análise qualitativa. De acordo com Laurence Bardin, para categorizar os elementos, é necessário identificar o que eles têm em comum e permitir que sejam agrupados (BARDIN, 1977). Por este âmbito é proposto realizar um recorte das abordagens semelhantes entre os entrevistados.

A AC lida com materiais em formato de textos escritos, diante disso, no desenvolvimento desta pesquisa, os áudios/ gravações das entrevistas foram transcritos para uma investigação minuciosa e detalhada.

Dessa forma, objetiva-se fazer uma coleta dos termos apresentados pelos entrevistados, de forma a realizar uma análise qualitativa. A entrevista e coleta das informações serão de caráter primário devido sua aplicação ser diretamente aos especialistas em segurança da informação. Através dos conceitos apresentados pelos participantes, objetiva-se fazer uma análise juntamente com o documento escrito, no caso a E-Ciber.

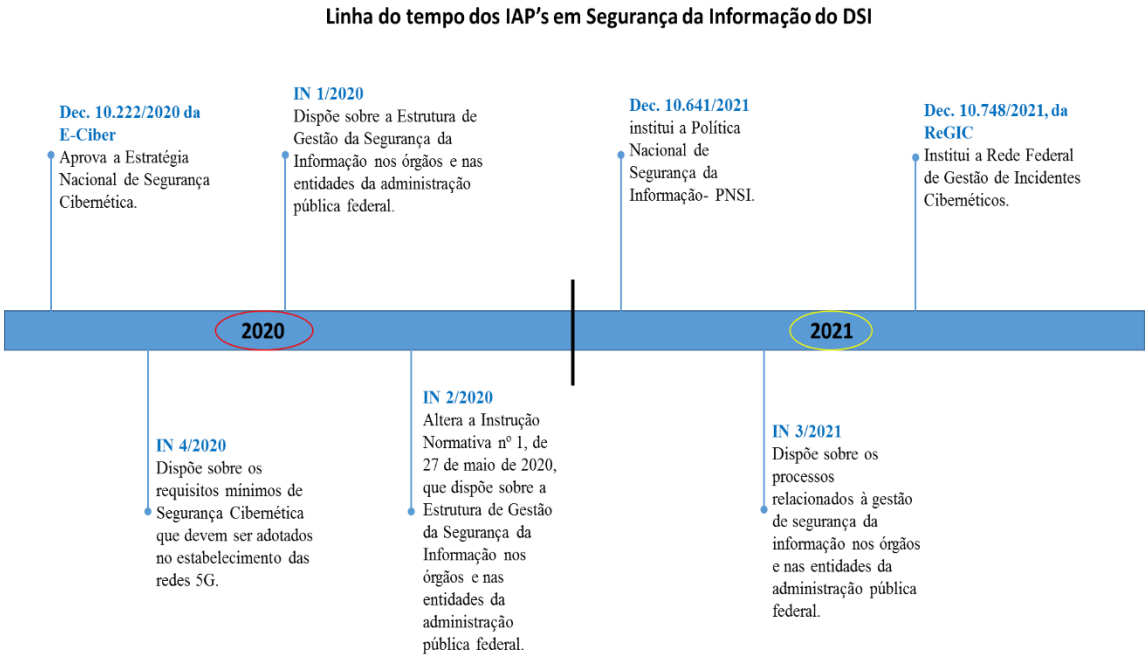
[2]Link: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 28 de janeiro de 2022.

4 CAPÍTULO ANALÍTICO

4.1 INSTRUMENTOS DE AÇÃO PÚBLICA EM SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO (DSI)

A linha do tempo abaixo dispõe sobre os instrumentos de ação pública do DSI nos períodos de fevereiro de 2020 a julho de 2021. A princípio, o intuito da pesquisa era abordar esses instrumentos desde julho de 2019; porém, diante de buscas e análises na página do DSI, foram encontradas iniciativas apenas a partir de fevereiro de 2020[3] no que tange aos instrumentos relacionados à segurança da informação e segurança cibernética.

Figura 1 — Linha do tempo dos Instrumentos de Ação Pública ligados ao tema da SI



Fonte: autoria própria.

Todos esses instrumentos de ação pública, que são regulamentações, decretos, instruções normativas, estabelecem requisitos, orientações, papéis e aperfeiçoamentos direcionados a cada órgão e entidade da APF direta e indiretamente nas ações relacionadas à Segurança da Informação.

[3] Representando um avanço em segurança da informação no período de julho de 2019 a julho de 2021.

O primeiro Decreto n° 10.222 abordado acima, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber)[4], apresenta a temática de SI de forma extensiva. Segundo este Decreto:

> A Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade. [5] (BRASIL, 2020a).

Nesta perspectiva, de acordo com o Decreto n° 10.222, a SI é distribuída por temáticas, ou seja, através da Estratégia Nacional de Segurança da Informação pretende-se contemplar todas as áreas em forma de módulos; dessa forma, a E-Ciber é apenas um módulo da área de Segurança Cibernética.

Segundo este instrumento de ação pública, a área de segurança cibernética[6] foi eleita a ser colocada no âmbito de discussão do primeiro módulo devido ser a área mais crítica e atual a ser abordada. Este Decreto aborda que a E-Ciber busca preencher uma importante lacuna no marco regulatório nacional de segurança cibernética, no qual essa Estratégia desenvolveu uma série de ações que visam modificar, de forma colaborativa, em nível nacional, características que refletem o posicionamento de instituições e indivíduos sobre o tema.

Já a Instrução Normativa (IN) n° 4, de 26 de março de 2020 (BRASIL, 2020b), aborda os requisitos mínimos de segurança cibernética que devem ser utilizados no estabelecimento das redes 5G. Esse instrumento de ação pública estabelece normas com o cumprimento obrigatório por parte das entidades e órgãos da APF, no qual são responsáveis pela implementação dessas redes de quinta geração. Nessa IN são abordados alguns conceitos em termos organizacionais com diretrizes a serem seguidas pela empresa prestadora de tal serviço. Segundo o artigo terceiro desta IN, as condições determinadas nesta IN tem o intuito de elevar a proteção da sociedade e das instituições nacionais, em decorrência da possibilidade de haver vulnerabilidades e backdoors[7] nos sistemas de tecnologias de quinta geração (BRASIL, 2020b).

Já a IN n° 01, de 27 de maio de 2020, diz respeito às orientações para gestão de SI no qual deverão ser observadas e implementadas pelos órgãos e entidades da APF, direta e indireta, com a finalidade de assegurar a disponibilidade, a confidencialidade, a integridade e

---

[4] Objetivos da E-Ciber serão expostos no item “4.2” desta pesquisa.

[5] Princípios mencionados por (FERNANDES, 2013) no Referencial teórico.

[6] Temática da SI.

[7] backdoor é uma porta de acesso ao sistema criada por um programa instalado que não é autorizado pelo proprietário do sistema, permitindo que pessoas não autorizadas tenham acesso ao computador.

a autenticidade da informação em âmbito nacional. Nesta IN são abordados alguns redirecionamentos para outros instrumentos de ação pública com o intuito de que os princípios da SI sejam seguidos (BRASIL, 2020d).

A IN n° 02, de 24 de julho de 2020, altera a IN n° 01 acima no requisito de cada órgão ou entidade deve ter uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), no qual essas equipes vão ser coordenadas pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) que se localiza na Presidência da República no Departamento de Segurança da Informação (BRASIL, 2020e).

Agora, serão abordados os instrumentos de ação pública publicados no ano de 2021. O Decreto n° 10.641, de 2 de março de 2021, altera o Decreto n° 9637, de 26 de dezembro de 2018, no qual institui a Política Nacional de Segurança da Informação (PNSI), a abordagem deste instrumento de ação pública traz novamente os princípios de SI e abordam alguns papéis do comitê gestor de segurança da informação, além de apresentar os papéis do Gabinete de Segurança Institucional relacionados a SI, que no caso um desses papéis é propor a versão do ato normativo necessário para implementar a PNSI (BRASIL, 2021a).

No entanto, a IN n° 03, de 28 de maio de 2021, prescreve processos relacionados à gestão da SI em órgãos e entidades da APF destinados na elaboração de seus planejamentos e implementações na temática de SI, no qual esses processos[8] devem ser de cumprimento obrigatório (BRASIL, 2021b).

Por fim, e não menos importante, até mesmo pelas evidências e resultados com as entrevistas na tabela a seguir, está o Decreto n° 10.748, de 16 de julho de 2021, no qual institui a Rede Federal de Gestão de Incidentes Cibernéticos, esta rede possui a finalidade de aperfeiçoar e manter a coordenação entre órgãos e entidades da APF para prevenção, tratamento e respostas a incidentes cibernéticos, com o intuito de elevar o nível de resiliência em segurança cibernética de seus ativos de informação, no qual a participação é obrigatória para os órgãos e entidades da APF direta, autárquica e fundacional. Nela são descritos alguns objetivos[9] no que se refere a sua operacionalidade (BRASIL, 2021c).

Diante de uma breve apresentação dos instrumentos de ação pública acima, torna-se fundamental trazer evidências encontradas nas entrevistas, evidências estas mencionadas

[8] Processos: I - mapeamento de ativos de informação; II - gestão de riscos de segurança da informação; III - gestão de continuidade de negócios em segurança da informação; IV - gestão de mudanças nos aspectos de segurança da informação; e V - avaliação de conformidade de segurança da informação.

[9] São objetivos da Rede Federal de Gestão de Incidentes Cibernéticos: I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos; II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas; III - divulgar informações sobre ataques cibernéticos; IV - promover a cooperação entre os participantes da Rede; e V - promover a celeridade na resposta a incidentes cibernéticos.

pelos gestores. A pergunta realizada foi: “Quais os principais avanços em SI no âmbito do DSI nos últimos anos desde julho 2019 até julho 2021? Ou seja, quais as normativas, ações governamentais e outros instrumentos que você destacaria como fundamentais para a preservação da SI no governo federal hoje?”[10] A partir daí, alguns gestores destacaram alguns instrumentos, apresentados abaixo:

Quadro 2 — Instrumentos de ação pública destacados pelos Gestores do DSI

Instrumentos de ação pública (IAP)	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**
Dec n° 10.222, 2020	X	X			X	X
IN n° 04, 2020	X	X				
IN n° 01, 2020						
IN n° 02, 2020						
Dec 10.641, 2021	X				X	X
IN n° 3, 2021						
Dec n° 10.748, 2021	X	X	X	X	X	
outros instrumentos	Dec 10.569[11]	Dec 10.569				

Fonte: autoria própria.

Todos esses instrumentos abordados no quadro acima foram abordados na linha do tempo anterior, com exceção do Decreto 10.569, de 9 de dezembro de 2020 (BRASIL, 2020f), que aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Esta regulamentação também é extremamente importante para a segurança da informação, tendo em vista que as áreas das infraestruturas críticas são campos prioritários, pois tratam de serviços essenciais para a sociedade. Quando uma dessas áreas sofre algum ataque cibernético, consequentemente as outras áreas também podem ser atingidas por ser um conjunto interdependente. Este instrumento não foi abordado na linha do tempo, por ser uma legislação correlata na página do DSI e não pertencer especificamente ao DSI.

Desta forma, diante da tabela exposta acima, os instrumentos de ação pública no qual foram mais destacados pelos seis gestores entrevistados são (em primeiro lugar) o Decreto n°

[10] Pergunta n° 2, localizada no Apêndice A desta pesquisa- Roteiro de entrevista.
[11] Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.

10.748 (BRASIL, 2021c), que institui a Rede Federal de Gestão de Incidentes Cibernéticos; em segundo lugar, o Decreto nº 10.222 (BRASIL, 2020a), no qual aprova a E-Ciber e, em terceiro, o Decreto nº 10.641 (BRASIL, 2021a), no qual altera o Decreto da Política Nacional de Segurança da Informação - PNSI.

Desta forma, esses instrumentos mais destacados representam avanços em segurança da informação e foram elencados como essenciais para a preservação da segurança da informação no governo federal.

4.2 OBJETIVOS ESTRATÉGICOS DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA (E-CIBER)

Os objetivos estratégicos da E-Ciber são direcionados por meio de orientações essenciais para que o setor público, setor produtivo e a sociedade possam desfrutar de um espaço cibernético confiável, resiliente, inclusivo e seguro. De acordo com o Decreto nº 10.222 (BRASIL, 2020a), no qual aprova a Estratégia Nacional de Segurança Cibernética, seus objetivos estratégicos são "1- Tornar o Brasil mais próspero e confiável no ambiente digital; 2- Aumentar a resiliência brasileira às ameaças cibernéticas e 3- Fortalecer a atuação brasileira em segurança cibernética no cenário internacional".

Para que esses objetivos sejam alcançados, algumas ações estratégicas são discorridas na E-Ciber, no qual se desdobra nas categorias abordadas a seguir. Essas categorias temáticas também foram identificadas nas entrevistas, ou seja, de certo modo, os argumentos levantados nas entrevistas relacionam-se com algumas ações estratégicas da E-Ciber.

4.2.1 Capacitação

A capacitação é algo essencial no espaço cibernético, pois o conhecimento na área é fundamental para introduzir medidas favoráveis em seu ambiente de trabalho ou até mesmo nas tarefas pessoais que envolvem a tecnologia.

No entanto, existem poucas pessoas especializadas em segurança cibernética. O Decreto nº 10.222 menciona uma pesquisa que foi realizada em 2018 pela empresa ManpowerGroup 62, porta-voz mundial em soluções inovadoras de força de trabalho. Possui cerca de quarenta mil empregadores de quarenta e três países. A empresa identificou que praticamente a metade deles (45%) tem adversidades para achar pessoas competentes, até mesmo - ou inclusive - na parte de segurança cibernética. No que tange aos empregadores

brasileiros, 34% declararam possuírem dificuldades em recrutar talentos (MANPOWER GROUP, 2018). Além do mais, de acordo com o Decreto nº 10.222, de 5 de fevereiro de 2020:

> As maiores dificuldades das empresas no processo de contratação no Brasil são a ausência de habilidades técnicas (33%), seguida pela falta de experiência (23%) e pela carência de habilidades interpessoais (19%). A primeira tem a ver com as lacunas educacionais brasileiras. (MANPOWER GROUP, 2018).

Como mencionado acima, a maior dificuldade no que tange à contratação é a ausência de habilidades técnicas, voltadas justamente para uma maior especialidade no assunto, no qual vão ser compreendidos por meio de formação acadêmica, cursos, livros, entre outros. Vários entrevistados relataram dificuldades em encontrar profissionais especializados na área de segurança cibernética. Um deles mencionou essa dificuldade, como pode ser observado no trecho a seguir:

> É difícil você encontrar um especialista em segurança cibernética porque é um curso caro, altamente especializado, onde se exigem muitos anos de estudo, treinamentos muito caros de caráter excepcional. Em meu antigo órgão, as provas eram dificílimas, o curso era na faixa de milhares de dólares, tipo mil dólares para cima, então para você encontrar um investimento ou uma disposição da alta administração para poder formar o especialista é muito difícil, então vejo que cada vez mais é difícil de encontrar um profissional que trabalha nesta área. (ENTREVISTADO 3, 2022).

Por este âmbito, percebe-se uma possível ausência de investimento em conhecimento e recursos para o servidor por parte da alta administração. Desta forma, um dos caminhos resolutivos seria a disposição governamental em investir em cursos e treinamentos de segurança cibernética para o indivíduo servidor da alta administração.

No que diz respeito à ausência de habilidades técnicas como resultado das lacunas educacionais, o Decreto nº 10.222, de 5 de fevereiro de 2020, da E-Ciber ainda traz uma conceituação da capacitação inclusa na educação:

> A capacitação engloba a educação, na modalidade profissional e tecnológica, destinada ao ensino continuado para profissionais da área, ou para aqueles cujo cargo ou função requeira conhecimentos técnicos mais profundos e especializados em segurança cibernética. A capacitação é a forma de atuação mais especializada e pode ser realizada por intermédio de treinamentos de curta duração, certificações de segurança, dentre outros meios. (BRASIL, 2020a).

Nesta abordagem, a capacitação é mencionada em uma vertente direcionada à educação no que tange à especialização por meio de cursos, treinamentos, certificados; no entanto, de acordo com a vertente do entrevistado acima, existem obstáculos, como a ausência

de capital. Os altos custos dos treinamentos em segurança cibernética tornam-se um empecilho para formar e capacitar profissionais nesta área.

Ainda, no que se refere à educação, durante as entrevistas, outro entrevistado mencionou que o maior problema no Brasil, no que se refere à segurança cibernética é a educação:

> A maior deficiência brasileira é em educação, não temos o hábito de preocuparmos com a segurança, não há uma valorização de senha, de backup, não se valoriza a segurança no trâmite de documentos físicos, todas essas argumentações, não estou falando apenas da alta administração, mas sim da sociedade brasileira, jogam documento para ser descartado de qualquer maneira no lixo, então tudo isso mostra claramente que nós precisamos educar a sociedade para a segurança, no nosso caso de segurança da informação e de segurança cibernética. (Entrevistado 5, 2022)

Recentemente, uma pesquisa realizada pelo *Center for Strategic and International Studies da Mcafee* confirma essas falhas levantadas neste tópico desta pesquisa denominado capacitação. Segundo esta pesquisa, as lacunas apontadas no Brasil são poucos profissionais especializados em segurança cibernética, poucos projetos educacionais focalizados na área e baixo entendimento dos usuários nesta temática. (MCAFEE, 2016).

4.2.2 Dimensão normativa e Arcabouço Legal

Uma das ações estratégicas da E-Ciber é aperfeiçoar o arcabouço legal sobre segurança cibernética. No entanto, elaborar normas para o espaço cibernético pode ser um desafio significativo devido ao rápido desenvolvimento que é a área tecnológica. O Decreto nº 10.222 que estabelece a E-Ciber aborda essa questão:

> Estabelecer normas e eventuais leis que rejam o espaço cibernético é sempre um desafio significativo, em razão do rápido desenvolvimento da tecnologia da informação e comunicação e dos sistemas de controle. Nesse sentido, é fundamental a ação coordenada entre as organizações governamentais e a sociedade em geral para prosseguir nos avanços legislativos sobre o tema. (BRASIL,2020a).

Nesta perspectiva, devido ao fato de o arcabouço legal nem sempre caminhar na mesma velocidade da tecnologia, se torna, também, fundamental o papel das instituições e sociedade. Tais funções são justamente nas ações de boas práticas em investir na segurança das informações corriqueiras de seu dia a dia.

Durante as entrevistas, alguns gestores de segurança da informação abordaram a importância das normas; para uma boa efetividade e efeito dessas regulamentações, eles

relataram que se torna primordial a conscientização dos cidadãos[12] em boas práticas de segurança da informação. Em uma das entrevistas, ao questionar o gestor se os instrumentos em formato de decretos, normas e outros têm sido suficientes em termos de resultados no que tange a segurança cibernética, o entrevistado relata:

> (…) o que acontece, a segurança da informação para se tornar eficaz, não depende apenas de normativo; sempre falamos que é um conjunto de coisas no qual envolve vários fatores; todos que trabalham nesta área de segurança da informação sabem que as boas práticas caracterizam que não apenas a área de TI que deve se preocupar com a segurança da informação e sim todas as partes interessadas de uma organização, por exemplo. Não adianta nada implementar um sistema de controle em segurança da informação se no meio de uma descontração na copa alguém informe um assunto sigiloso, então é uma coisa que tem que partir do senso de cultura organizacional e de conscientização dos cidadãos, no qual vai muito além, um normativo ajuda a conscientizar, a informar, porém sua execução exige uma série de outros fatores. (Entrevistado 3, 2022)

Nesta perspectiva, a conscientização é um elemento fundamental, seja por parte dos integrantes da APF, seja por parte dos demais atores da sociedade. Para a Estratégia Nacional de Segurança Cibernética (E-Ciber) atingir um de seus objetivos, que, no entanto, é aprimorar o arcabouço legal nas temáticas de segurança cibernética, se torna em vão este aperfeiçoamento se as ações práticas não condizem com os requisitos básicos implementados nos instrumentos de ação pública.

[12] Essa conscientização são os “outros fatores” no Apêndice B (Arcabouço: dimensão normativa) desta pesquisa.

4.2.3 Educação em segurança cibernética na base comum curricular

Como discutido nos tópicos acima, um dos desafios encontrados em segurança cibernética foi à dificuldade de encontrar pessoas especializadas no assunto. No entanto, a raiz do problema pode estar na ausência de conhecimento na temática desde o início, na base comum curricular. Sem conhecimento do que é segurança cibernética e de como aplicá-la em seu cotidiano, dificilmente o estudante terá interesse por este assunto. Nesta perspectiva, o Decreto que estabelece a Estratégia Nacional de Segurança Cibernética afirma:

> A abordagem da segurança cibernética nas escolas brasileiras ainda é muito incipiente, quando não, inexistente. No âmbito da educação superior, a segurança cibernética, como disciplina ou programa de estudo, ainda é de difícil acesso aos alunos. (BRASIL, 2020a)

Para reafirmar esta abordagem acima, durante as entrevistas, os gestores relataram essa problemática; em específico, a ausência de capacitação direcionada a todos os graus de ensino, um deles abordou afirmou que "não existe um curso na área acadêmica que prepare uma pessoa para trabalhar na área de segurança cibernética, então se torna importante uma política pública de capacitação desde o ensino fundamental" (Entrevistado 4, 2022).

Nesta perspectiva de políticas públicas, é de fundamental importância uma parceria do governo com o Ministério da Educação (MEC) para articular e implementar políticas públicas nesta temática. A E-Ciber menciona um exemplo de divergência dos projetos das universidades em consonância com as demandas de segurança cibernética no setor produtivo e recomenda:

> O estabelecimento de parcerias com o Ministério da Educação, visando à implementação de programas de incentivo ao desenvolvimento de capacidades em segurança cibernética para estudantes da educação básica, com o objetivo de identificar talentos, e orienta-se que as universidades desenvolvam projetos em alinhamento com as necessidades do setor produtivo. (BRASIL, 2020a)

Desta forma, percebe-se que a educação em segurança cibernética para os estudantes em todos os níveis – do ensino fundamental ao superior – pode gerar um futuro rentável para vários setores que necessitam da segurança cibernética, incluindo, como destacado acima, o setor produtivo e o governamental.

Investir em projetos de leis e políticas públicas para implementação do ensino em segurança cibernética na educação básica torna-se um dos caminhos resolutivos para ter uma futura sociedade evoluída e com conhecimento sobre segurança da informação.

Durante as entrevistas, um dos gestores mencionou que uma das metas principais para o Departamento de Segurança da Informação (DSI) nos próximos anos é criar um Projeto de Lei no qual a segurança cibernética seja implementada obrigatoriamente em todos os graus de ensino. Ele afirma que:

> Nosso objetivo principal é mandar para o congresso um projeto de lei da segurança cibernética, ou seja, a Política Nacional de Segurança Cibernética (PNSC) que poderá nos atribuir competência para um gerenciamento nacional da segurança cibernética. A minuta já está pronta e ela cita o Ministério da Educação (MEC), porque nós queremos que a segurança cibernética seja assunto obrigatório em todos os graus de ensino. (Entrevistado 5, 2022).

5 CONSIDERAÇÕES FINAIS

Ao iniciar este projeto de pesquisa, constatou-se que a SI é um ativo importante para distintos atores, seja para o governo, sociedade, setor financeiro e para as áreas das infraestruturas críticas nos requisitos de manter a própria ordem nacional. Diante desta perspectiva, a dúvida de como o governo federal brasileiro estava tratando esta temática foi à pergunta norteadora da pesquisa. Por este âmbito, surgiu o tema deste projeto, que aborda as políticas públicas de segurança da informação na prevenção e tratamento de incidentes cibernéticos.

As dúvidas de como o governo federal estipula e implementa políticas públicas na área de SI através dos instrumentos de ação pública foram sanadas através do Departamento de Segurança da Informação, localizado na Presidência da República (PR) durante todo o delineamento desta pesquisa acadêmica.

Para o esboço de toda a pesquisa, este estudo teve como objetivo geral identificar alguns avanços e desafios na temática da Segurança da Informação no governo federal brasileiro. Constata-se que este objetivo geral foi alcançado através do mapeamento dos instrumentos de ação pública, no qual foram encontrados instrumentos especificamente na temática de SI a partir de 2020, representando um avanço nestes últimos anos. E com uma análise discursiva e conjunta das entrevistas juntamente com a E-Ciber foram identificados alguns desafios.

Através da coleta dos instrumentos de ação pública, o intuito a princípio era identificar estes instrumentos do Departamento de Segurança da Informação a partir de julho de 2019. No entanto, tais instrumentos foram encontrados somente a partir de 2020, no qual evidencia um avanço e mais discussões a partir deste ano de 2020. O instrumento de ação pública que ocupou o primeiro lugar, no qual os gestores mais destacaram como fundamental para a SI e prevenção de incidentes cibernéticos, foi a Rede Federal de Gestão de Incidentes Cibernéticos (Decreto n° 10.748).

Através de uma análise da Estratégia Nacional de Segurança Cibernética (E-Ciber) juntamente com as entrevistas, conclui-se que os principais desafios em SI, no qual inclui a segurança cibernética é encontrar trabalhadores especializados e capacitados na área de segurança cibernética, inclusive um dos desafios especificamente do DSI que todos os gestores relataram foi a necessidade de trabalhadores no departamento, ou seja, há um efetivo reduzido. Além disso, a metade dos entrevistados relatou que os instrumentos de ação pública por si só não são suficientes para a solução dos problemas públicos em segurança da

informação, pois depende de outros fatores que ainda devem ser trabalhados, como a conscientização do cidadão para seguir caminhos favoráveis de segurança durante o seu cotidiano. Por fim, tanto a E-Ciber como os gestores nas entrevistas levantaram argumentos a favor da aprendizagem em segurança cibernética ser essencial em todos os graus de ensino da base comum curricular.

REFERÊNCIAS

AGUIAR *et al*. **O Governo Eletrônico:** aspectos gerais sobre a modernização administrativa da gestão pública brasileira. [Brasil]: [s.n.], 2018.

ALBUQUERQUE, Bruno Marques; SILVA, Fernanda Cláudia Araújo; SOUSA, Thanderson Pereira De. A era eletrônica da administração pública federal. **Revista Vianna Sapiens**, v. 8, 2017.

ANGROSINO, M. **Etnografia e observação participante.** Porto Alegre: Penso, 2009.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1977.

BAUER, Martin W.; GASKELL, George. **Pesquisa qualitativa com texto, imagem e som:** um manual prático. [S.l.]: Editora Vozes Limitada, 2017.

BRASIL. **Decreto n° 9.573, de 22 de novembro de 2018.** Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Palácio do Planalto, 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9573.htm. Acesso em: 23 ago. 2021.

BRASIL. **Decreto n° 9.668, de 2 de janeiro de 2019a**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão. Brasília, DF: Palácio do Planalto, 2019. Disponível em: www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9668.htm. Acesso em: 26 ago. 2021.

BRASIL. **Lei n° 13.844, de 18 de junho de 2019b**. Estabelece a organização básica dos Órgãos da Presidência da República e dos Ministérios. Brasília, DF: Palácio do Planalto, 2019. Disponível em: www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13844.htm. Acesso em: 26 ago. 2021.

BRASIL. **Decreto n° 10.222, de 5 de fevereiro de 2020a**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 23 jan. 2022.

BRASIL. **Instrução Normativa n° 4, de 26 de março de 2020b**. Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468. Acesso em: 29 jan. 2022.

BRASIL. **Decreto n° 10.363, de 21 de maio de 2020c.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão. DSI/PR. Brasília, DF: Palácio do Planalto, 2020. Disponível em: www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10363.htm. Acesso em: 26 ago. 2021.

BRASIL. **Instrução Normativa n° 01, de 27 de maio de 2020d**. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 29 jan. 2022.

BRASIL. **Instrução Normativa n° 02, de 24 de julho de 2020e.** Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700. Acesso em: 31 jan. 2022.

BRASIL. **Decreto 10.569, de 9 de dezembro de 2020f**. Aprova a Estratégia Nacional de Infraestruturas Críticas. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357. Acesso em: 2 fev. 2022.

BRASIL. **Decreto n° 10.641, de 2 de março de 2021a.** Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Brasília, DF: Palácio do Planalto, 2020. Disponível em:https://www.in.gov.br/en/web/dou/-/decreto-n-10.641-de-2-de-marco-de-2021-306212181. Acesso em: 31 jan. 2022.

BRASIL. **Instrução Normativa n° 03, de 28 de maio de 2021b.** Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 31 jan. 2022.

BRASIL. **Decreto n° 10.748, de 16 de julho de 2021c.** Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, DF: Palácio do Planalto, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022#:~:text=Institui%20a%20Rede%20Federal%20de%20Gest%C3%A3o%20de%20Incidentes%20Cibern%C3%A9ticos.&text=DE%20INCIDENTES%20CIBERN%C3%89TICOS-,Art.,26%20de%20dezembro%20de%202018. Acesso em: 31 jan. 2022.

CANONGIA *et al*. **Guia de referência para a seguranças das infraestruturas críticas da informação.** Versão 01, nov. 2010. Disponível em: https://livroaberto.ibict.br/bitstream/1/607/2/GUIA%20DE%20REFER%C3%8ANCIA%20PARA%20A%20%20SEGURAN%C3%87A%20DAS%20INFRAESTRUTURAS%20CR%C3%8DTICAS%20DA%20INFORMA%C3%87%C3%83O.pdf. Acesso em: 11 ago. 2021.

CAREGNATO, Rita *et al*. Pesquisa qualitativa: análise de discurso versus análise de conteúdo. **Texto & Contexto - Enfermagem**, [*s.l.*], v. 15, n. 4, p. 679-684, dez. 2006. FapUNIFESP (SciELO). Disponível em: http://dx.doi.org/10.1590/s0104-07072006000400017.

CDN/SE. **Portaria Nº 34, de 5 de agosto de 2009**. Conselho de Defesa Nacional, Secretaria Executiva. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação. CGSI: Brasília, 2009.

CRISPIM, Renata. **Participação cidadã digital:** análise de instrumentos de ação pública do governo federal brasileiro sobre governança digital e governo digital. [Brasil]: [*s.n.*], 2021.

de Lima, T. C. S. *et al* (2007). A documentação no cotidiano da intervenção dos assistentes sociais: algumas considerações acerca do diário de campo. **Textos & Contextos (Porto Alegre), 6**(1), 93-104.

FERNANDES, N. (2013) **Segurança da Informação**. Cuiabá- MG, Instituto Federal Rondônia. Disponível em: http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1. Acesso em: 19 ago. 2021.

FONTES, Edison. **Segurança da informação,** o usuário faz a diferença**.** 1ª edição. São Paulo: Saraiva, 2006.

FOUNTAIN, Jane. Central issues in the political development of the virtual state. **The Network Society From Knowledge to Policy**, v. 149, 2005.

FOUNTAIN. Disjointed Innovation: The Political Economy of Digitally Mediated Institutional Reform. **NCDG working paper**, 2011. Disponível em: http://works.bepress.com/jane_fountain/93. Acesso em: 26 ago. 2021.

GARTNER GROUP. Key issues in E-Government Strategy and Management. **Research Notes**, Key issues, 23 maio 2000.

HALL, P. A.; TAYLOR, R. C. R. As três versões do neo-institucionalismo. **Lua Nova**, n.58, p.193-223, 2003. Disponível em: https://www.scielo.br/j/ln/a/Vpr4gJNNdjPfNMPr4fj75gb/?format=pdf. Acesso em: 26 ago. 2021.

HECKERT; AGUIAR, 2016. **Governança digital da administração pública federal:** uma abordagem estratégica para tornar o governo digital mais efetivo e colaborativo- a ótica da sociedade. Disponível em: http://consad.org.br/wp-content/uploads/2016/06/Painel-32-01.pdf. Acesso em: 10 set. 2021.

CASTELLS, M.; CARDOSO, G. **The Network Society**: From Knowledge to Policy. Brookinga Institution Press: Washington-DC, 2006.

INFORMA BR. **Segurança da informação**. Norma ISO/IEC 17799:2000. Disponível em: https://www.informabr.com.br/nbr.htm. Acesso em: 19 ago. 2021.

KLIMBURG, Alexander. **National Cyber Security Framework Manual**, NATO CCD COE Publication. Tallin, 2012. Disponível em: https://rainydaydragon.files.wordpress.com/2016/01/nationalcybersecurityframeworkmanual.pdf . Acesso em: 11 ago. 2021.

KRAEMER, K.; KING, J. Information Technology and Administrative Reform: Will e-government be Different? **International Journal of Electronic Government Research**, v. 2, n. 1, p. 1-20, jan-mar, 2006.

LASCOUMES, Pierre; LE GALÈS, Patrick. A ação pública abordada pelos seus instrumentos. Revista Pós Ciências Sociais, v. 9, n. 18, 2012.

LAVILLE, Christian. DIONNE, Jean. **A construção do saber:** manual de metodologia da pesquisa em ciências humanas. Porto Alegre: Penso, 1999.

MANPOWER GROUP**. SKILLS REVOLUTION 2.0**. Disponível em: https://www.manpowergroup.com/wps/wcm/connect/59db87a7-16c6-490d-ae70-1bd7a322c240/Robots_Need_Not_Apply.pdf?MOD=AJPERES. Acesso em: 3 fev. 2022.

MARCH, J. OLSEN, J. **Rediscovering Institutions**. Londres: Macmillan, 1989.

MCAFEE — Center for strategic and international studies. **Hacking the skills shortage: a study of the international shortage in cybersecurity skills**. Jul 2016. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf. Acesso em: 4 fev. 2022.

MINAYO, M.C. de S. **O desafio do conhecimento:** pesquisa qualitativa em saúde. São Paulo - Rio de Janeiro: HUCITEC-ABRASCO, 1992. Disponível em: https://www.scielo.br/j/csc/a/FgpDFKSpjsybVGMj4QK6Ssv/. Acesso em: 11 ago. 2021.

NORTH. D. C. Institutions, **Institutional Change and Economic Performance**. Cambridge: Cambridge University Press, 1990.

OLIVEIRA, Marcos A. G.; PAGLIARI, Graciete D. C.; MARQUES, Adriana A.; PORTELA, Lucas S. e FERREIRA NETO, W. B. **Guia de Defesa Cibernética na América do Sul.** Recife: Ed. UFPE, 2017.

OLIVEIRA, Nairobi; GOMES, Moises; LOPES, Ronaldo; NOBRE, Jéferson. **Segurança da Informação para internet das coisas (IoT):** uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). 2019. Disponível em: https://sol.sbc.org.br/journals/index.php/reic/article/view/1704/1553. Acesso em: 12 ago. 2021.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: https://jus.com.br/artigos/3186. Acesso em: 23 ago. 2021.

Revista Pós Ciências Sociais, Maranhão, v. 9, n. 18, 2012. Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/rpcsoc/article/viewFile/1331/1048. Acesso em: 11 ago. 2021.

SÊMOLA, M. (2014) **Gestão de segurança da informação:** uma visão executiva**.** 2.ed. Rio de Janeiro: Elsevier. Disponível em: http://wiki.stoa.usp.br/images/archive/7/79/20170827173359%21Cap1-semola.pdf. Acesso em: 11 ago. 2021.

SETI (Soluções em Tecnologia). **Incidentes Cibernéticos -** O que são e como se proteger. Jaraguá do Sul-SC, 13 de janeiro de 2020. Disponível em: https://www.seti.com.br/incidentes-ciberneticos-o-que-sao-e-como-se-proteger/. Acesso em: 11 ago 2021.

SILVA; NOGUEIRA. **Ataques cibernéticos e medidas governamentais para combatê-los,** 2019. Disponível em: ebrevistas.eb.mil.br/OC/article/view/2127. Acesso em: 11 ago. 2021.

APÊNDICES

Apêndice A — Roteiro de entrevista em pesquisa acadêmica para os Gestores de segurança da informação no Departamento de Segurança da Informação (DSI)

1. Qual sua função/ cargo/ contribuição nas atividades de Segurança da Informação (SI) dentro do (DSI)?
2. Quais os principais avanços em SI no âmbito do DSI nos últimos anos desde julho 2019 até julho 2021? Ou seja, quais as normativas, ações governamentais e outros instrumentos que você destacaria como fundamentais para a preservação da SI no governo federal hoje?
3. Qual o papel do DSI para a SI e prevenção de incidentes cibernéticos no governo federal?
4. Os instrumentos, leis e políticas que temos hoje são suficientes para obtenção de resultados e soluções em SI e no tratamento de incidentes cibernéticos?
5. Quais os principais desafios em SI no âmbito do DSI hoje?

Apêndice B — Folha de sumário codificado (Entrevistas)

Item	Código	Referência	Pergunta	Quantidade de evidências
Capacitação	CAPTÇ	De acordo com o Decreto 10.222, 5 de fev de 2020[13]: A capacitação engloba a educação, na modalidade profissional e tecnológica, destinada ao ensino continuado para profissionais da área, ou para aqueles cujo cargo ou função requeira conhecimentos técnicos mais profundos e especializados em segurança cibernética. A capacitação é a forma de atuação mais especializada e pode ser realizada por intermédio de treinamentos de curta duração, certificações de segurança, dentre outros meios.	Quais os principais desafios em SI[14] no âmbito do DSI hoje?	Efetivo reduzido (todos os entrevistados); Necessidade de expandir o DSI (todos os entrevistados); Ausência de encontrar profissionais na área (3); Ausência de programas de treinamento (3); Necessidade de uma estrutura física mais robusta (3); Necessidade de implementar e receber equipamentos (3); Necessidade de implementar o videowaal[15] (1);
Arcabouço: dimensão normativa	ACDN	De acordo com o Decreto 10.222, 5 de fev de 2020: Estabelecer normas e eventuais leis que rejam o espaço cibernético é sempre um desafio significativo, em razão do rápido desenvolvimento da tecnologia da informação e comunicação e dos sistemas de controle. Nesse sentido, é fundamental a ação coordenada entre as organizações governamentais e a sociedade em geral para prosseguir nos avanços legislativos sobre o tema.	Os instrumentos, leis e políticas que temos hoje são suficientes?	Não são suficientes devido a temática de segurança cibernética estar em constante evolução e depender de outros fatores[16] (3); Suficientes, mas tem muito a melhorar, além da temática depender de outros fatores além das normas (2); Suficientes (1); Necessidade de ampliar o espectro normativo (1);
Educação em segurança cibernética na base comum curricular	EDSCBC	De acordo com o Decreto 10.222, 5 de fev de 2020: A abordagem da segurança cibernética nas escolas brasileiras ainda é muito incipiente, quando não, inexistente. No âmbito da educação superior, a segurança cibernética, como disciplina ou programa de estudo, ainda é de difícil acesso aos alunos.	Os instrumentos, leis e políticas que temos hoje são suficientes?	Necessidade de implementar o conhecimento em segurança da informação[17] na base comum curricular (1); Necessidade de uma política pública de capacitação desde o ensino fundamental (1); Necessidade de um projeto de lei que direcione o assunto de segurança cibernética a ser assunto obrigatório em todos os graus de ensino (1);

[13] https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

[14] Segurança da Informação, no qual abrange a temática de segurança cibernética.

[15] Rede de telas computacionais para exibir informações, propagandas e entretenimentos.

[16] Como a conscientização dos usuários/ cidadãos que utilizam a internet.

[17] Segurança da informação abrange a segurança cibernética, pois a segurança cibernética é uma área temática da segurança da informação.