



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE EDUCAÇÃO / CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
MESTRADO PROFISSIONAL EM GESTÃO EM ORGANIZAÇÕES
APRENDENTES

JOSÉ ROBERTO CAVALCANTE DA SILVA

ESTUDOS PROSPECTIVOS SOBRE O CIBER TERRORISMO NA PARAÍBA

João Pessoa
2018

JOSÉ ROBERTO CAVALCANTE DA SILVA

ESTUDOS PROSPECTIVOS SOBRE O CIBER TERRORISMO NA PARAÍBA

Dissertação apresentada à banca de defesa do Programa de Pós-Graduação em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito institucional para obtenção do Título de Mestre.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

Linha de Pesquisa: Gestão de Projetos Educativos e Tecnologias Emergentes

João Pessoa

2018

Catálogo na publicação
Seção de Catalogação e Classificação

S586e Silva, José Roberto Cavalcante da.
Estudos prospectivos sobre o Ciber Terrorismo na
Paraíba / José Roberto Cavalcante da Silva. - João
Pessoa, 2018.
106 f. : il.

Orientação: Wagner Junqueira de Araújo.
Dissertação (Mestrado) - UFPB/CE.

1. Gestão nas Organizações. 2. Segurança da informação.
3. Tecnologias da Informação e Comunicação. 4. Ciber
Terrorismo. 5. Cenários prospectivos - Godet. I.
Araújo, Wagner Junqueira de. II. Título.

UFPB/BC

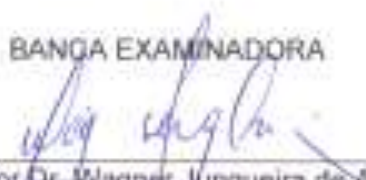
JOSÉ ROBERTO CAVALCANTE DA SILVA

ESTUDOS PROSPECTIVOS SOBRE O CIBER TERRORISMO NA PARAÍBA

Dissertação apresentada à banca de defesa do Programa de Pós-Graduação em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito institucional para obtenção do Título de Mestre.

Aprovada em: 23, maio, 2018

BANCA EXAMINADORA



Professor Dr. Wagner Junqueira de Araújo
Orientador (UFPB)

Professor Dr. Marcikson Roberto Ferreira de Sousa
Examinador Interno (UFPB)



Professora Dra. Julianne Teixeira e Silva
Examinador Externo (UFPB)

Professora Dra. Izabel França de Lima
Examinador Interno Suplente (UFPB)

Professor Dr. Henry Poncio Cruz de Oliveira
Examinador Externo Suplente (UFPB)

RESUMO

A informação adquiriu a condição de ativo nas organizações públicas ou privadas na sociedade da informação. Percebe-se que a utilização das tecnologias da informação e da comunicação pelas instituições potencializou e elevou a sua competitividade, proporcionando rapidez e celeridade de transmissão e processamento da informação. Da mesma maneira, as ameaças à segurança da informação destacam-se na proporção em que surgem formas mais sofisticadas de ataques aos ativos informacionais, como o terrorismo cibernético, objeto deste estudo. Esta pesquisa apresentou como objetivo prospectar cenários sobre o ciber terrorismo na Paraíba. Foram consultados como amostra intencional por conveniência da pesquisa órgãos públicos e empresas que sofreram ataques ou ameaças de ataques descritas na mídia como sendo ciber terrorismo no período de janeiro de 2016 até o ano de 2017. Para tanto, realizou-se uma investigação de natureza qualiquantitativa, bibliográfica e descritiva, empregando o método de construção de cenários prospectivos de Godet. Na etapa do exame dos dados, os instrumentos utilizados foram: análise estrutural; Método de Atores, Objetivos, Relações de força; e a análise morfológica. Essas ferramentas são específicas do método de Godet, que recebe auxílio de *softwares*. Apresentou-se como resultado um diagnóstico da situação da segurança da informação e do ciber terrorismo em organizações da Paraíba. Identificaram-se as seguintes variáveis: políticas públicas; ideologias; mercado; tecnologias e vantagem indevida. Outrossim, apontaram-se os atores a seguir: governo; empresas; colaboradores; clientes/usuários e pessoas externas. Por fim, foram desenvolvidos os seguintes cenários possíveis para o ciber terrorismo na Paraíba: cenário propício; cenário adverso; e cenário provável. O primeiro foi exposto como um cenário favorável para a realização de ataques de natureza ciber terrorista no âmbito das organizações estudadas. O segundo foi apresentado como um cenário desfavorável para a atuação do ciber terrorismo no contexto analisado. O terceiro mostra um crescimento gradativo dos ataques de cunho ciber terrorista na conjuntura das instituições investigadas.

Palavras-chave: Gestão da Segurança da Informação. Tecnologias da Informação e da Comunicação. Ciber Terrorismo. Cenários Prospectivos.

ABSTRACT

Information has acquired the status of asset in public or private organizations in the information society. It is perceived that the use of information and communication technologies by institutions has potentiated and increased its competitiveness, providing speed and celerity of transmission and information processing. Likewise, threats to information security stand out as more sophisticated forms of attacks on information assets, such as cyber-terrorism, the subject of this study, emerge. This research aimed to prospect scenarios about cyber terrorism in Paraíba. Public agencies and companies that have suffered attacks or threats of attacks described in the media as cyber terrorism from January 2016 to 2017 have been consulted as an intentional sample for the convenience of the research. For this, an investigation of qualitative and quantitative nature, bibliographical and descriptive, was carried out, using Godet's method of prospective scenarios. At the data analysis stage, the instruments used were: structural analysis; Actors Method, Objectives, Strength Relationships; and morphological analysis. These tools are specific to Godet's method, which is aided by software. As a result, a diagnosis of the information security and cyber-terrorism situation in Paraíba organizations was presented. The following variables were identified: public policies; ideologies; market; technologies and undue advantage. Also, the following actors were pointed out: government; companies; contributors; customers / users and external people. Finally, the following possible scenarios for cyber terrorism in Paraíba were developed: a favorable scenario; adverse scenario; and probable scenario. The first one was exposed as a favorable scenario for the accomplishment of attacks of cyber terrorist nature within the organizations studied. The second was presented as an unfavorable scenario for cyber terrorism in the analyzed context. The third shows a gradual increase in cyber terrorist attacks in the conjuncture of the investigated institutions.

Keywords: Information Security Management. Information and Communication Technologies. Cyber Terrorism. Prospective Scenarios.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CAIS	Centro de Atendimento a Incidentes de Segurança
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CNAM	<i>Conservatoire National des Arts et Métiers</i>
CTIR Gov	Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
GSI	Gestão da Segurança da Informação
LIPS	<i>Laboratory of Investigation in Prospective and Strategy</i>
MACTOR	Método de Atores, Objetivos, Relações de força
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MICMAC	Matriz de Impactos Cruzados - Multiplicações Aplicadas a uma Classificação
MPPB	Ministério Público da Paraíba
PDCA	<i>Plan</i> (planejar), <i>Do</i> (fazer), o <i>Check</i> (cheçar) e o <i>Act</i> (agir).
PDCL	<i>Plan</i> (planejar), o <i>Do</i> (fazer), o <i>Check</i> (cheçar) e o <i>Learn</i> (aprender).
PWC	PricewaterhouseCoopers
RNP	Rede Nacional de Ensino e Pesquisa
SI	Segurança da Informação
TI	Tecnologia da Informação
TICs	Tecnologias da Informação e da Comunicação
TRT13	Tribunal Regional do Trabalho da 13ª Região

LISTA DE FIGURAS

Figura 1 – Estrutura Textual da Dissertação	20
Figura 2 – Mapa conceitual da síntese das ideias centras deste capítulo.....	45
Figura 3 – Elementos do Ciber terrorismo.....	53
Figura 4 – Matriz de influências diretas das variáveis no aplicativo MICMAC.....	73
Figura 5 – Mapa de influências/dependências diretas das variáveis.....	74
Figura 6 – Matriz de influências diretas dos atores no aplicativo MACTOR.....	77
Figura 7 – Mapa de influências e dependências entre atores	78
Figura 8 – Matriz de posições valoradas entre atores e objetivos.....	79
Figura 9 – Matriz de posições simples entre atores e objetivos	79
Figura 10 – Mapa de convergências entre atores	80
Figura 11 – Histograma da implicação dos atores sobre os objetivos.....	81

LISTA DE GRÁFICOS

Gráfico 1 – Total de incidentes reportados ao CERT.br por ano.....	17
Gráfico 2 – Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2016	60
Gráfico 3 – Distribuição de incidentes por categoria	62
Gráfico 4 – Influências diretas das variáveis	75
Gráfico 5 – Convergências entre atores.....	81

LISTA DE QUADROS

Quadro 1 – Motivos dos ataques cibernéticos.....	15
Quadro 2 – Classificação de ameaças em grupos segundo sua intencionalidade	37
Quadro 3 – Exemplos de vulnerabilidades	38
Quadro 4 – Princípios essenciais da segurança da informação	41
Quadro 5 – Ataques Reportados ao CERT.br	61
Quadro 6 – Número, variável, abreviatura e descrição no MICMAC	73
Quadro 7 – Número, ator, abreviatura e descrição no MACTOR	76
Quadro 8 – Número, objetivo, abreviatura e descrição no MACTOR	77
Quadro 9 – Ações para a gestão da segurança da informação das organizações ...	88

LISTA DE TABELAS

Tabela 1 – Análise da ordem da ameaça mais comum no contexto organizacional .	68
Tabela 2 – Análise da ordem da motivação de um ataque ciber terrorista.....	69
Tabela 3 – Análise da ordem das medidas de proteção e combate aos ataques ciber terroristas	70

SUMÁRIO

1 INTRODUÇÃO	13
1.1 JUSTIFICATIVA	15
1.2 OBJETIVOS	19
1.3 ESTRUTURA TEXTUAL DA DISSERTAÇÃO	20
2 PERCURSO METODOLÓGICO	22
2.1 CARACTERIZAÇÃO DA PESQUISA	23
2.2 UNIVERSO, POPULAÇÃO E AMOSTRA DA PESQUISA	25
2.3 MÉTODO DA PESQUISA	25
2.4 TÉCNICA DA COLETA E ANÁLISE DE DADOS	28
3 REVISÃO DA LITERATURA	34
3.1 GESTÃO DA SEGURANÇA DA INFORMAÇÃO	34
3.2 CIBER TERRORISMO	46
3.2.1 Terrorismo: conceitos e aspectos gerais	46
3.2.2 Ciberespaço	48
3.2.3 Terrorismo Cibernético ou ciber terrorismo	51
3.2.4 Ativismo no ciberespaço ou Ciber ativismo	56
3.2.5 Tipos de ataques no Brasil	59
4 ANÁLISE DOS DADOS E RESULTADOS	65
4.1 DELIMITAÇÃO DO SISTEMA E DO AMBIENTE ESTUDADO	65
4.2 IDENTIFICAÇÃO E ANÁLISE DAS VARIÁVEIS E DOS ATORES	71
4.2.1 Análise estrutural das variáveis	72
4.2.2 Análise da relação de atores	75
4.3 CONSTRUÇÃO DOS CENÁRIOS POSSÍVEIS APLICADOS AO CIBER TERRORISMO NA PARAÍBA.....	82
5 CONSIDERAÇÕES FINAIS	85
REFERÊNCIAS.....	90
APÊNDICE A – Termo de Consentimento Livre e Esclarecido (TCLE)	97

APÊNDICE B – Formulário para a Coleta de Dados	99
ANEXO A – PARECER CONSUBSTANCIADO DO COMITÊ DE ÉTICA.....	103

1 INTRODUÇÃO

No contexto da globalização, nota-se uma transformação nas relações sociais e econômicas, é possível visualizar uma ruptura com os padrões tradicionais de relacionamento interpessoal, em que os povos passam a estar integrados, vinculados e relacionados. Ou seja, percebe-se uma proposta de aproximação, união, celeridade e totalidade, em âmbito internacional. Isso proporciona uma natureza complexa para a sociedade vigente, que também recebe a denominação de sociedade da tecnologia, da informação, do conhecimento, entre outras, devido ao viés valorativo e estratégico desses termos no contexto organizacional.

No coração da globalização está a velocidade acelerada em que as atividades ocorrem. Isto contém várias implicações: a mais aparente delas é a quebra de fronteiras geográficas ou territoriais, em que a informação é transmitida através do mundo, e indivíduos podem participar no mesmo evento ao mesmo tempo, independentemente de sua localização geográfica. O único requisito para participação é o acesso à Internet. (ANG; PANG, 2014, p. 50).

Dessa forma, a globalização pode ser considerada um sistema de desenvolvimento, que apresenta impactos positivos ou negativos em dimensões distintas. Para este trabalho o foco será na dimensão informacional, as demais como a econômica, a social e a tecnológica servirão somente como suporte para a proposta desta pesquisa.

Entre os impactos positivos, percebe-se que a informação passou a ser disseminada, por meio da internet, de qualquer lugar do mundo com rapidez e presteza, pois não há mais limites territoriais. Além disso, existe uma relação estreita entre a informação e as tecnologias da informação e da comunicação (TICs) no âmbito das organizações, que atribui valor para a informação.

O uso da informação pelas organizações é considerado um dos recursos mais importantes para garantir a competitividade nos dias atuais. A informação é criada, tratada e transferida às organizações, sendo a eficiência desse processo a garantia do bom desempenho e do deslocamento da organização para patamares mais elevados de competitividade. (CALAZANS, 2006, p. 64).

A informação organizacional possui um enfoque estratégico na medida em

que busca agregar valor para bens ou serviços da organização, assegurando a sua sobrevivência neste contexto atual, desafiador e competitivo. Da mesma forma, a informação permite reduzir as incertezas durante a tomada de decisão, propiciando escolhas adequadas e com risco reduzido. (CALAZANS, 2006).

“A informação é um ativo da organização, talvez o mais precioso, um bem que deve ser tão protegido quanto os bens físicos, tendo em vista a sua importância para a própria existência da organização.” (MANOEL, 2014, p. 2).

Nessa perspectiva, verifica-se a relevância da informação, considerando-a um ativo essencial para a manutenção dos negócios de uma organização, que precisa de uma adequada proteção e conservação.

Por outro lado, negativamente, a partir da globalização, houve o desenvolvimento dos perigos, dos riscos e das ameaças, relacionados aos recursos da informática, como: vazamentos de informações, fraudes, falhas, entre outros. As ameaças passaram a utilizar instrumentos mais sofisticados para explorar as vulnerabilidades das tecnologias da informação e da comunicação, que são empregadas de maneira expressiva nesse contexto, e causar, sobretudo, prejuízos financeiros para pessoas físicas e organizações públicas ou privadas.

Segundo Albahar (2017), houve um aumento significativo da ocorrência de ataques virtuais em todo o mundo. Estes ataques acontecem, por exemplo, na forma de invasões maliciosas, suspensão temporária de serviços, violação de dados, atividades de espionagem, etc. Neste ambiente instável, grupos terroristas passaram a explorar o espaço cibernético de maneira célere como mais um canal para disseminar suas mensagens, criando um cenário de insegurança e medo.

Conforme estes grupos evoluem para o ciberespaço, a Gestão de Segurança da Informação tem sua atuação dificultada, pois está diante de novas ameaças, como: ciber ativismo; ciber terrorismo; entre outras. Essas ameaças apresentam em comum a realização de ataques contra computadores por meio do ciberespaço, contudo a intenção ou motivação difere. Neste estudo, o objeto será o fenômeno do terrorismo cibernético ou ciber terrorismo.

O terrorismo cibernético é uma ameaça em desenvolvimento no século XXI, tornando a segurança da informação em ambientes cibernéticos necessária para que as organizações possam proteger seus ativos. (ALBAHAR, 2017). Tais ameaças apresentam riscos potenciais, porém ainda não é possível encontrar uma definição ou padrões comuns, o que prejudica a tomada de decisão do Gestor de Segurança

da Informação em relação aos ataques de ciber terroristas.

Diante dessas exposições, este estudo busca responder a seguinte questão de pesquisa: **Como estão os cenários sobre o ciber terrorismo na Paraíba?**

1.1 JUSTIFICATIVA

Essa indagação de pesquisa emergiu da necessidade de um entendimento mais adequado acerca do ciber terrorismo, fenômeno ligado às tecnologias da Informação e da comunicação, na Paraíba, que é uma ameaça à segurança da informação em potencial, e explora as vulnerabilidades das tecnologias para provocar diversos prejuízos.

Em relação à intenção dos ataques cibernéticos, nota-se que as motivações são diversas, em que as com propósito de obter vantagem financeira e as de cunho ideológico são as que mais se enquadram como ações de ciber terroristas. O quadro 1 descreve as principais motivações de ataques virtuais.

Quadro 1 - Motivos dos ataques cibernéticos

Motivo	Descrição
Demonstração de poder	“mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.”
Prestígio	“vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar <i>sites</i> considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.”
Motivações financeiras	“coletar e utilizar informações confidenciais de usuários para aplicar golpes.”
Motivações ideológicas	“tornar inacessível ou invadir <i>sites</i> que divulguem conteúdo contrário a opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.”
Motivações comerciais	“tornar inacessível ou invadir <i>sites</i> e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.”

Fonte: Adaptado de CERT.br (2012, p. 17-18).

Em relação aos ataques cibernéticos, o relatório do ano de 2013 da RNP – Rede Nacional de Ensino e Pesquisa informa os principais incidentes de segurança de informação, que acontecem no referido ano na rede acadêmica do Brasil, destacando o crescimento expressivo de ataques de negação de serviço (*DDoS*) e a diminuição no quantitativo geral de incidentes no ano, que são reportados ao CAIS – Centro de Atendimento a Incidentes de Segurança, comparado a 2012. O Relatório lista os seguintes incidentes em destaque no ano de 2013: código malicioso na forma de *Bot* e *Botnet*; tentativa de exploração de vulnerabilidades, que está relacionada a *scan*; fraude na forma de *Phishing*; conteúdo abusivo por meio da técnica de *Spam*; e ataques de negação de serviço (*DDoS – Distributed Denial of Service*). (RNP, 2013).

No período de maio a agosto de 2015, os incidentes em destaque foram o *Ransomware* e *Stagefright*. O primeiro é um golpe em ascensão, que age como um sequestrador de arquivos digitais. Nesse golpe, os arquivos sequestrados são cifrados e a vítima é conduzida ao pagamento de um resgate através de transferência bancária ou *bitcoins*. O segundo trata de uma vulnerabilidade no Android. (RNP, 2015).

No primeiro semestre de 2017, o *Ransomware* volta a ser destaque, ratificando o seu aumento significativo anualmente. Nesse período, o *Ransomware* causou uma das maiores crises virtuais de nível global, provocando grandes prejuízos, inclusive em órgãos públicos e em instituições da rede de ensino e pesquisa do Brasil. (RNP, 2017).

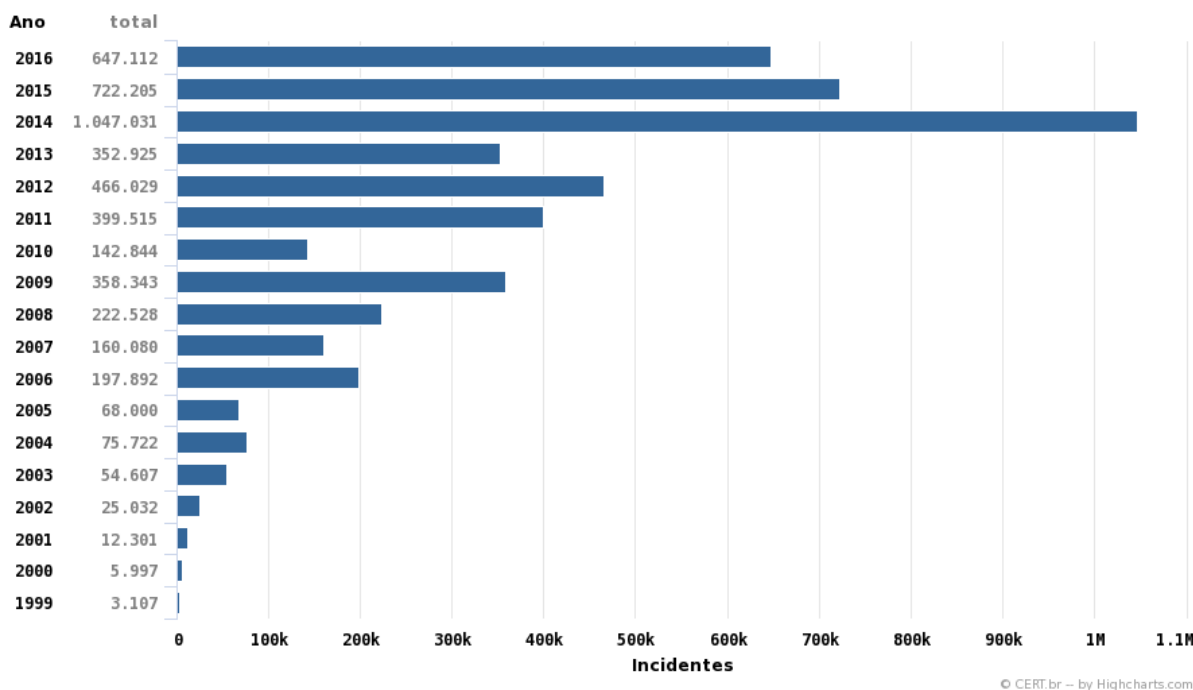
Percebe-se que houve um aumento gradativo de ataques cibernéticos nos últimos anos. Os meios de ataque também estão evoluindo, tornando-se mais qualificados e enérgicos.

Os números são estarrecedores. Ano após ano, os ataques cibernéticos seguem crescendo em frequência, gravidade e impacto. Os métodos de prevenção e detecção mostram-se muito ineficazes contra investidas cada vez mais sofisticadas. Muitas organizações não sabem o que fazer, ou não têm os recursos necessários para combater criminosos cibernéticos altamente qualificados e agressivos. (PWC, 2016, p. 4).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) também apresenta a possibilidade de acompanhar, anualmente, o

aumento ou o declínio dos incidentes de segurança cibernética no Brasil, indicados no gráfico 1.

Gráfico 1 - Total de incidentes reportados ao CERT.br por ano



Fonte: CERT.br (2016).

Verifica-se que há uma diminuição de incidentes de segurança informados ao CERT.br, comparando os anos 2014, que houve um crescimento exagerado, 2015 e 2016. Isso pode significar que a área de segurança da informação evoluiu, no sentido de controlar alguns ataques cibernéticos, ou que os ataques se tornaram mais sofisticados e não estão sendo detectados, ou, ainda, que não estão sendo reportados ao CERT.br. Todavia, ainda, existe um número expressivo de registro dos ataques anuais por meio da internet, requerendo atenção da gestão da segurança da informação.

No Brasil, o ciber terrorismo, ainda, é um evento novo e a literatura especializada não apresenta uma definição clara ou precisa sobre o termo. É notória a falta de conhecimento e ausência de dispositivos para reduzir e inibir essa ameaça. Isso ficou evidente através dos ataques ciber terroristas de proporções mundiais, que ocorreram no dia 12 de maio de 2017 e prejudicaram o funcionamento de empresas e órgãos públicos de diversos países do mundo, incluindo o Brasil.

Na Paraíba, alguns órgãos públicos, como o Tribunal Regional do Trabalho da 13ª Região (TRT13) e o Ministério Público da Paraíba (MPPB), tiveram a ruptura do princípio da disponibilidade, devido ao referido ataque. Essas afirmações foram constatadas na mídia, sendo que fragmentos de notícia exemplifica e trata do

ataque:

O ataque *hacker* que atingiu 99 países nesta sexta-feira não tem precedente na história do cibercrime. Menos de 24 horas depois de identificado, já atingiu mais de 75.000 computadores e servidores ao redor do mundo. As instruções que aparecem na tela das vítimas foram preparadas em 28 idiomas diferentes, inclusive português. Todo esse planejamento e execução, realizados com precisão, dependem da existência de uma infraestrutura específica, investimento e organização.

[...]

Os *hackers* utilizaram uma brecha do sistema Windows para codificar os computadores atingidos, tornando-os inacessíveis para os usuários. Depois exigiram o pagamento de resgates no valor de 300 dólares (cerca de 940 reais) para desfazer a criptografia. Sem o código em poder dos bandidos, é impossível reaver os dados.

[...] No Brasil, dezenas de empresas foram atingidas, apesar de nenhuma assumir publicamente. Em diversos locais, os funcionários foram orientados a desligar os computadores como medida de precaução, para evitar o ataque. (VEJA, 2017).

Percebe-se que os ciber terroristas potencializaram suas formas de ataques virtuais. Da mesma forma, os terroristas cibernéticos exploram vulnerabilidades para realizar seus ataques, como foi ratificado nos fragmentos acima da notícia da revista Veja, mostrando que houve a exploração de uma fragilidade no sistema Windows.

Nesse contexto, a sofisticação dos ataques virtuais fica evidente nos seguintes trechos de uma notícia que aborda esta temática:

O maior ataque cibernético norte-coreano foi realizado em setembro de 2016, quando a rede interna do comando militar sul-coreano foi infectada por um vírus informático. O Ministério da Defesa da Coreia do Sul confirmou a informação só em maio passado. Durante o ataque foram roubados cerca de 235 gigabytes de dados militares, uma quantidade equivalente a 15 milhões de páginas de documentos.

Os hackers norte-coreanos conseguiram inserir um código malicioso no software fornecido pela empresa de segurança informática do Exército da Coreia do Sul, comunicou Lee Cheol-hee, advogado do Partido Democrata da Coreia do Sul. (SPUTNIK, 2017).

Nota-se que os trechos acima confirmam a capacidade dos ciber terroristas de causarem grandes prejuízos aos sistemas de informação.

Nesse cenário, a busca por uma compreensão apropriada do terrorismo cibernético justifica-se pois possibilita criar mecanismos de proteção que reduza a sua atuação sob a informação de organizações públicas ou privadas. Este estudo se

justifica pois possibilita subsidiar a tomada de decisão estratégica da área de gestão da segurança da informação, no sentido de promover modelos para defesa adequada contra o ciber terrorismo.

Nessa perspectiva, este estudo está relacionado ao Programa de Pós-Graduação em Gestão nas Organizações Aprendentes, em que se encontra inserido na linha de pesquisa Gestão de Projetos Educativos e Tecnologias Emergentes, apresentando uma natureza de processo educativo em relação à proteção contra o fenômeno Ciber terrorismo. Além disso, este estudo destaca a Gestão na área da Segurança da Informação, que é essencial para a Gestão das Organizações com foco na aprendizagem.

Para tanto, optou-se por uma metodologia de construção de cenários prospectivos acerca do ciber terrorismo na Paraíba, utilizando o método proposto por Michel Godet.

O método prospectivo faz uma reflexão para explicar a ação de cunho estratégico, em que antecipa cenários futuros para influenciar a atividade estratégica. (GODET, 2000). Para os autores “[...] um cenário é um conjunto formado pela descrição de uma situação futura e pela cadeia de acontecimentos que permitem passar da situação de origem à situação futura.” (GODET; DURANCE, 2011, p. 26).

Essa metodologia trabalha e prioriza os acontecimentos incertos do mundo. Dessa forma, ela é coerente para este estudo sobre o ciber terrorismo, tendo em vista que se trata de um evento de características indeterminadas.

Assim, os argumentos expostos acima ratificam e fundamentam a relevância deste estudo para o contexto organizacional. Propõe-se identificar elementos para que as organizações do estado da Paraíba se planejem de forma a minimizar os impactos de possíveis novos ataques. Nessa perspectiva, esta pesquisa terá seu processo conduzido para o alcance dos seguintes objetivos:

1.2 OBJETIVOS

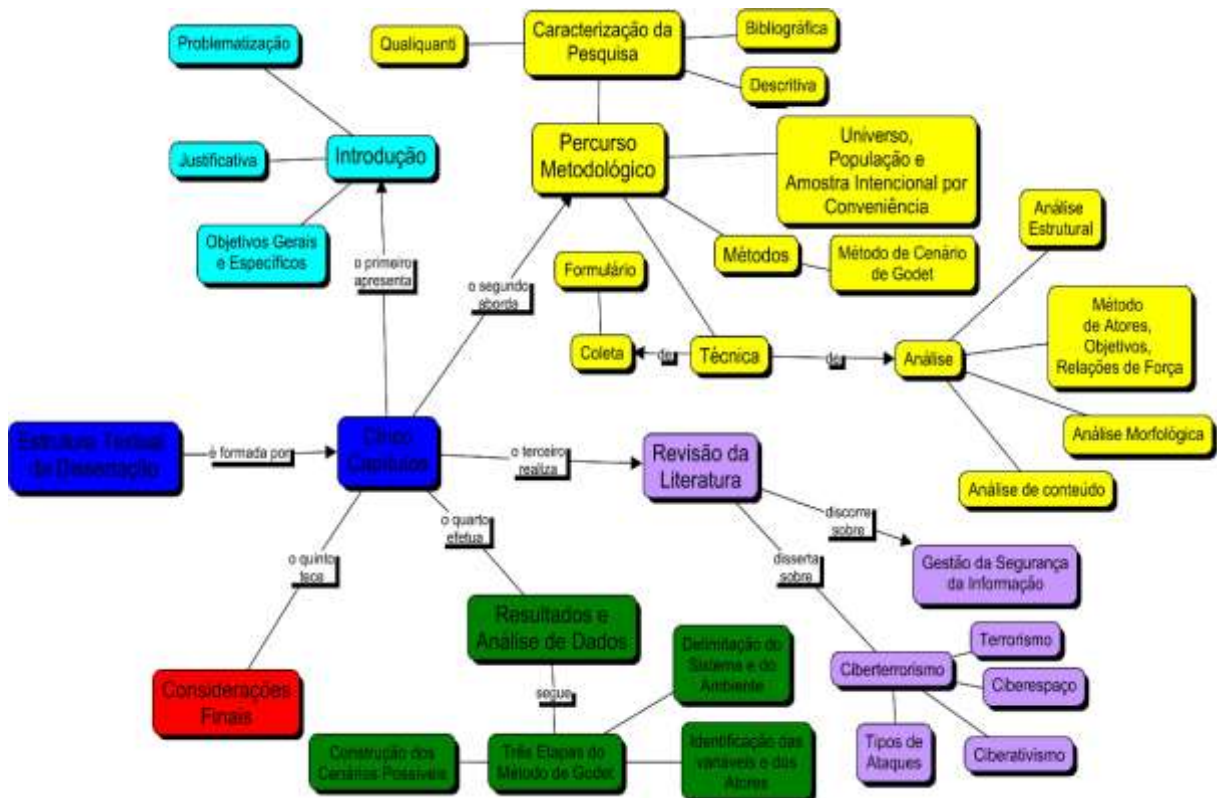
Esta pesquisa tem-se como objetivo geral **estudar cenários prospectivos sobre o ciber terrorismo na Paraíba**. Para atingir este objetivo geral, pretende-se desenvolver os seguintes objetivos específicos:

- Identificar as variáveis-chave e os atores do ciber terrorismo em organizações públicas ou privadas da Paraíba;
- Examinar a interação das variáveis e dos atores;
- Elaborar cenários prospectivos para o ciber terrorismo na Paraíba;
- Propor ações para gestão da segurança da informação com base nos cenários desenvolvidos.

1.3 ESTRUTURA TEXTUAL DA DISSERTAÇÃO

Esta dissertação será formada por cinco capítulos, conforme ilustra a figura 1 que representa a estrutura textual da dissertação.

Figura 1 – Estrutura Textual da Dissertação



Fonte: Elaborada pelo autor (2017).

O primeiro capítulo apresenta a introdução, que é composta pela problematização, justificativa, objetivo geral e objetivos específicos. O segundo capítulo aborda o percurso metodológico, que trata da caracterização da pesquisa como “qualiquantitativa”, bibliográfica e descritiva. Da mesma forma, indica o universo, a população e a amostra intencional por conveniência, bem como apresenta o método de cenário de Godet e as técnicas de coleta e análise de dados:

formulário; análise estrutural; método de atores, objetivos, relações de força; análise morfológica; e análise de conteúdo, empregados na pesquisa.

O terceiro capítulo realiza uma revisão de literatura, em que, inicialmente, discorre sobre a Gestão da Segurança da Informação. Em seguida, disserta-se acerca do Ciber terrorismo, em que se discutem os temas: terrorismo; ciberespaço; terrorismo cibernético; ciber ativismo; por fim, apresenta os tipos de ataques identificados no Brasil.

O quarto capítulo efetua a descrição dos resultados e a análise dos dados, orientadas pelas três etapas principais do método apontadas por Godet: **delimitação do sistema e do ambiente estudado; identificação das variáveis e dos atores; construção dos cenários prospectivos possíveis**. O quinto capítulo tece as considerações finais da pesquisa e sugere as ações de segurança.

2 PERCURSO METODOLÓGICO

A metodologia é o percurso do pensamento e a prática realizada no contexto real. Ou melhor, abrange, concomitantemente, os métodos, as técnicas ou instrumentos e a criatividade do pesquisador (sua experiência, sua habilidade particular e sua percepção). (DESLANDES; GOMES; MINAYO, 2009).

Dessa maneira, a metodologia pode ser definida como: aglomerado de métodos e técnicas usados em uma pesquisa; o itinerário a ser cumprido para alcançar o objetivo; a maneira de resolver problemas, buscando respostas adequadas para as dúvidas e necessidades; forma de dirigir uma investigação; preocupa-se com instrumentos; trata dos procedimentos, das técnicas; conhecimento geral e as capacidades que são essenciais ao pesquisador. (MICHEL, 2009).

Este estudo utilizará a metodologia proposta por Michel Godet para desenvolver cenários prospectivos sobre o terrorismo cibernético ou ciber terrorismo na Paraíba e sugerir ações para segurança da informação.

O método de construção de cenários busca construir representações do futuro, assim como rotas que levam até essas representações. Essas representações buscam destacar as tendências dominantes e as possibilidades de ruptura no ambiente em que estão localizadas as organizações e instituições. Cenários representam uma excelente opção, pois constituem uma forma de integração com outras informações úteis e são excelentes para comunicar resultados aos usuários em geral. (SANTOS *et al*, 2004, p. 212).

Os cenários podem ser classificados em exploratórios e antecipatórios ou normativos. Os primeiros mostram as tendências pregressas e as atuais, e o prolongamento em tendências futuras. Os cenários antecipatórios, por sua vez, são produzidos a partir de percepções alternativas de futuros, apontando cenários desejados e cenários que devem ser evitados. (SANTOS *et al*, 2004).

Os estudos de cenários prospectivos diferem da previsão de futuro e analisam o mundo de incertezas em um período de longo prazo, mostrando e estudando as várias probabilidades de futuros aceitáveis, preparando e adaptando as organizações para enfrentar as mudanças do meio. Além disso, esses estudos produzem situações que diminuem os impactos dos eventuais cenários futuros.

(MORITZ; PEREIRA, 2005).

A análise de cenários se caracteriza como o estudo criativo ou imaginativo sobre o futuro com abordagem e metodologia próprias. Permitindo às organizações não só criar seus cenários futuros, como também, ao longo do desdobramento das suas cenas e trajetórias, construir respostas rápidas às mudanças do ambiente. (MORITZ; NUNER; PEREIRA, 2008, p. 70).

Os cenários de larga escala colaboram na produção de estratégias e investimentos, possibilitam melhores decisões a partir da identificação de incertezas, aumentam a compreensão acerca do âmbito externo, e ampliam a celeridade de respostas a fenômenos imprevisíveis através da visualização antecipada de prováveis futuros. (WRIGHT; SILVA; SPERS, 2010).

Neste capítulo, mostra-se o caminho a ser percorrido para atingir os objetivos e responder à pergunta problema deste estudo.

2.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa é a atividade essencial da ciência, que denota a realidade. Ou seja, é um evento de busca de conhecimento não definitivo, pois há mais o que descobrir. A pesquisa científica apresenta a proposta de explorar, descrever e explicar o mundo físico. (MICHEL, 2009).

Marconi e Lakatos (2010) mostram que a pesquisa pode ser concebida como um processo formal com procedimento de entendimento reflexivo que solicita um tratamento científico, estabelecendo-se no trajeto para se aprender a realidade ou para encontrar fatos incompletos. Além disso, a pesquisa descobre respostas para indagações propostas, empregando métodos científicos.

Nessa perspectiva, esta pesquisa apresenta uma natureza qualitativa-quantitativa, pois quantificará os dados coletados, analisando-os de forma qualitativa.

Considera-se como “qualiquanti” (importante instrumento da pesquisa social) a pesquisa que quantifica e percentualiza opiniões, submetendo seus resultados a uma análise crítica qualitativa. Isso

permite levantar atitudes, pontos de vista, preferências que as pessoas têm a respeito de determinados assuntos, fatos de um grupo definido de pessoas. Permite identificar falhas, erros, descrever procedimentos, descobrir tendências, reconhecer interesses, identificar e explicar comportamentos. (MICHEL, 2009, p. 39).

Além disso, a pesquisa pode ser classificada quanto aos meios e quanto aos fins. Em relação aos meios ou procedimentos, esta pesquisa pode ser compreendida como bibliográfica. Michel (2009) afirma que se trata da primeira etapa da pesquisa, em que se busca a relação de bibliografias sobre o assunto, com a intenção de observar informações e subsídios para definir objetivos, o problema e os pontos do referencial teórico.

Neste sentido, a pesquisa bibliográfica é fundamental para execução da primeira etapa proposta por Godet, que trata do recenseamento das variáveis e atores.

Pizzani *et al.* (2012) compreendem que a pesquisa bibliográfica é uma revisão da literatura sobre as principais teorias que orientam a pesquisa científica. Ou melhor, é denominado levantamento bibliográfico ou revisão bibliográfica, que pode ser por meio de livros, periódicos, artigo de jornais, sites da Internet, entre outros.

Desse modo, este estudo realizará um levantamento por meio de consultas no Portal de Periódicos CAPES, em que serão usados os seguintes termos chaves na língua portuguesa: **segurança da informação; terrorismo; ciberespaço; ciber terrorismo; e ciber ativismo**. Serão consultados também periódicos na língua inglesa, em que os termos chaves da busca são: **information security; terrorism; cyberspace; cyberterrorism; e cyberactivism**. Além de outras fontes de pesquisa bibliográfica, que serão apontadas nas referências.

Em relação aos fins ou aos objetivos, esta pesquisa pode ser classificada como descritiva. Michel (2009) afirma que a pesquisa de natureza descritiva verifica e explica problemas, fenômenos ou fatos da realidade, observando e realizando conexões com o ambiente.

“Trata, em geral, de levantamentos das características de uma população, um fenômeno, um fato, ou o estabelecimento de relações entre variáveis controladas.” (MICHEL, 2009, p. 44).

Dessa maneira, esta pesquisa descreverá, verificará e explicará o fenômeno

ciber terrorismo, apresentando conceitos, características e estabelecendo relações com o âmbito externo, sobretudo com outros eventos como o ciber ativismo. E elaborando os cenários prospectivos sobre o tema na Paraíba.

2.2 UNIVERSO, POPULAÇÃO E AMOSTRA DA PESQUISA

O **universo** desta pesquisa será os órgãos públicos e as empresas do Estado da Paraíba, que sofreram ataques ou ameaças de ataques do terrorismo cibernético no período de janeiro de 2016 até o ano de 2017.

A **população** deste estudo será constituída pelos servidores e os empregados do setor de Tecnologia da Informação (TI) dos órgãos públicos e de empresas do Estado da Paraíba que se habilitarem a participarem da pesquisa.

A **amostra** desta pesquisa será na forma **intencional por conveniência**, ou seja, utilizará servidores ou empregados do setor de TI de **8 (oito)** organizações, que se disponibilizarem a participarem da pesquisa. Dessa forma, foram selecionados **16 (dezesesseis) participantes**, sendo **2 (dois)** de cada setor que autorizou a coleta dos dados. Nesse sentido, participaram da pesquisa **12 (doze)** servidores públicos de **6 (seis)** órgãos públicos distintos, **2 (dois)** empregados públicos de uma empresa pública e **2 (dois)** trabalhadores de uma organização privada. Pressupõe-se que estas organizações por meio de seus representantes auxiliem na construção de cenários sobre o terrorismo cibernético na Paraíba.

2.3 MÉTODO DA PESQUISA

O método pode ser compreendido como um sistema, um processo organizado, um aglomerado de técnicas ordenadas, empregadas para alcançar o produto desejado. Ou seja, é o projeto geral, que orienta o procedimento, é o percurso e a forma selecionada para alcançar o resultado esperado. (MICHEL, 2009).

Assim, o método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo –

conhecimentos válidos e verdadeiros – traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista. (MARCONI; LAKATOS, 2010, p. 65).

Nessa perspectiva, esta pesquisa utilizará o método de cenário de Michel Godet para a construção de cenários prospectivos acerca do terrorismo cibernético.

Godet (2000), professor principal de prospectiva do *Conservatoire National des Arts et Métiers* (CNAM) e diretor do *Laboratory of Investigation in Prospective and Strategy* (LIPS), em Paris na França, afirma que há uma caixa de ferramentas para os estudos prospectivos e para os estudos estratégicos, os quais estão, estreitamente, vinculados e devem ser apreendidos por todos os atores organizacionais. Além disso, esse autor mostra que as incertezas do ambiente justificam a emergência da construção de cenários para a evolução estratégica e sustentável das organizações em um longo prazo.

O referido autor emprega a expressão “caixa de ferramentas” para se referir aos instrumentos usados no planejamento de cenários prospectivos, os quais apresentam as seguintes vantagens: estimula a imaginação; reduz as inconsistências; cria uma linguagem e um pensamento comum; possibilita a apropriação pelos tomadores de decisão.

Santos *et al* (2004) mostram que o método de construção de cenários é constituído por algumas propostas básicas como: explicar as práticas do presente a partir do futuro; investigar futuros diversos e indefinidos; adotar uma perspectiva universal e sistemática; considerar os aspectos qualitativos e as técnicas dos atores; optar por enfoques múltiplos e complementares; entre outras.

Percebe-se que as ideias de Santos *et al* (2004) vão ao encontro do método de cenários de Godet, no sentido em que procuram compreender as ações presentes a partir de situações futuras.

Para Godet (2000), não há uma perspectiva singular sobre os métodos de cenários prospectivos. Não obstante, esses métodos podem ser compreendidos como a descrição de uma situação futura e do encaminhamento de fenômenos, que viabilizam o desenvolvimento de uma situação inicial para os cenários futuros. Os cenários podem ser classificados em exploratórios e antecipatórios ou normativos. O primeiro parte de tendências passadas e presentes para situações futuras. O segundo baseia-se em percepções alternativas do futuro, podendo ser desejáveis ou

receosos. Ele também afirma que o seu método possui três etapas centrais: identificar as variáveis-chave por meio de uma análise estrutural; analisar jogos de atores para fazer questionamentos sobre o futuro; e reduzir as incertezas e selecionar os cenários ambientais mais possíveis.

Este método é composto por nove etapas, que não possuem um desenvolvimento completamente sequencial, ou seja, não é necessário e obrigatório seguir uma ordem linear das etapas, pois, normalmente, não há tempo suficiente. Da mesma forma, a utilização do método será um sucesso se atender os seguintes pré-requisitos: relevância, importância, coerência, plausibilidade e transparência. (GODET, 2000).

Nessa perspectiva, seguem as nove etapas do método proposto pelo autor:

1. Analisar o problema e determinar o sistema de análise;
2. Realizar um raio X de toda a organização;
3. Identificar as principais variáveis internas e externas da organização através de uma análise estrutural;
4. Buscar entender o retrospecto de uma organização, identificando os aspectos vulneráveis e os positivos, e indicando as questões-chave para o futuro;
5. Reduzir as incertezas, destacar grandes tendências e deduzir os mais possíveis cenários;
6. Enfatizar as percepções, os projetos e as estratégias coerentes e adequadas com os cenários prováveis da organização;
7. Avaliar as estratégias, refletir antes da ação e da tomada de decisão;
8. Estimular o desafio, considerando a tomada de decisão;
9. Implementar o plano de ação, gerando um acompanhamento e um desenvolvimento contínuo.

Desta forma, “o método dos cenários visa construir representações dos futuros possíveis, bem como das sequências de acontecimentos que a eles conduzem.” (GODET; DURANCE, 2011, p. 48).

Godet e Durance (2011) apresentam uma proposta de método de cenários, que possuem apenas três etapas: construir a base; varrer o campo dos possíveis e reduzir a incerteza; e elaborar os cenários. A primeira fase consiste na produção de um aglomerado de representações da situação atual do sistema, que envolve distintos elementos do contexto organizacional. Esta base é uma reunião de variáveis relacionadas entre si, que é construída por meio da definição do sistema,

das variáveis fundamentais e da apreciação das estratégias dos atores. A segunda etapa planeja os eventuais futuros mediante uma relação de hipóteses, que expressam a continuidade ou a ruptura de uma tendência. A terceira fase, por sua vez, descreve o encaminhamento que conduz os acontecimentos presentes para a situação futura.

Diante do exposto, este estudo utilizará as três etapas principais do método apontadas por Godet: **delimitação do sistema e do ambiente estudado; identificação das variáveis e dos atores; construção dos cenários prospectivos possíveis aplicados ao ciber terrorismo na Paraíba**, tendo em vista que não é obrigatório seguir todas as etapas do método, bem como as etapas referentes a elaboração das estratégias, tomada de decisão, implementação e controle do plano de ação ficam sob o critério e a responsabilidade dos gestores das respectivas organizações estudadas. No mais o tempo disposto para realização da pesquisa seria suficiente para desenvolver e analisar mais etapas.

2.4 TÉCNICA DA COLETA E ANÁLISE DE DADOS

A técnica é a ferramenta de execução do método, são as etapas a serem cumpridas, é a maneira específica de efetuar o método. As técnicas são dispositivos usados para coletar dados, sendo fundamentais para a integridade, a qualificação e a plenitude da pesquisa. O levantamento de dados, por sua vez, pode ser categorizado em primário ou de primeira mão, secundário e terciário. O primeiro ocorre através da pesquisa de campo, de entrevistas, de questionários, etc. O segundo acontece mediante análise de documentos, livros, revistas, entre outros. O terceiro realiza-se a partir da menção de outras pessoas, em que não houve o acesso para validação. (MICHEL, 2009).

Neste estudo, será utilizado **o formulário** para a coleta de dados primários em relação à construção de cenários prospectivos do ciber terrorismo na Paraíba, conforme modelo em apêndice B. Neste formulário, inicialmente, terá um breve esclarecimento do que se trata a pesquisa.

O formulário é um instrumento de coleta de dados constituído de uma lista formal de questões previamente elaboradas e ordenadas e voltadas para o propósito da pesquisa. Sua grande característica reside no fato de ser preenchido pelo pesquisador, preferencialmente na presença do pesquisado. No formulário, o pesquisador faz as perguntas, esclarece dúvidas, e registra, ele mesmo, as respostas, após criticá-las e adequá-las aos objetivos da pesquisa. Neste instrumento, a coleta deve ser feita, de preferência, individualmente, ou restrita a pequenos grupos para que a atuação do pesquisador possa ser mais efetiva. (MICHEL, 2009, p. 71).

Ressalta-se que esse instrumento de coleta de dados foi aplicado aos participantes após a emissão do parecer consubstanciado do Comitê de Ética da UFPB, que se encontra no anexo A desta dissertação. Além disso, a assinatura do participante e do pesquisador no Termo de Consentimento Livre e Esclarecido (TCLE), que se localiza no apêndice A, foi necessária para que o formulário pudesse ser empregado.

Para a análise, a descrição e a construção dos cenários, serão empregadas as três etapas do **método de cenário de Michel Godet**, conforme subseção anterior, em que os instrumentos serão: a **análise estrutural**, auxiliada pelo *software* Matriz de Impactos Cruzados - Multiplicações Aplicadas a uma Classificação (MICMAC)¹; o **Método de Atores, Objetivos, Relações de força** (MACTOR), auxiliado pelo *software* MACTOR²; e a **análise morfológica**.

A análise estrutural é um procedimento ordenado, apresentando uma tipologia matricial, de análise das relações entre as variáveis do sistema analisado e as do ambiente explicativo. Essa ferramenta objetiva fazer surgir as variáveis básicas, que são influentes e dependentes. Da mesma forma, faz emergir as variáveis fundamentais para o desenvolvimento do sistema estudado. Esse método é realizado mediante um conjunto de atores e especialistas que apresentam conhecimento considerável. A análise estrutural ocorre através de três etapas consecutivas: o recenseamento das variáveis, a descrição das relações entre variáveis e a identificação das variáveis-chave. A primeira etapa compreende o inventário do aglomerado das variáveis internas e externas, que compõem as características do sistema e do seu ambiente analisados. A segunda etapa busca

¹ Disponível em: <<http://pt.lapropective.fr/metodos-da-prospectiva/software/151-micmac.html>>. Acesso em: 08 de outubro de 2017.

² Disponível em: <<http://en.lapropective.fr/methods-of-prospective/software/60-mactor.html>>. Acesso em: 08 de outubro de 2017.

menção das relações efetivas entre as variáveis, empregando o quadro de dupla entrada, chamado de matriz de análise estrutural. (GODET; DURANCE, 2011).

Nota-se que análise das relações entre variáveis acontece por meio de um procedimento qualitativo. Dessa maneira, conforme Godet e Durance (2011, p. 64):

O preenchimento é qualitativo. Para cada par de variáveis, colocam-se as questões seguintes: existe uma relação de influência direta entre a variável i e a variável j ? Se a resposta for negativa, é atribuída a nota 0. Se a resposta for positiva, são atribuídas as seguintes notas à relação de influência direta: 1, se for considerada fraca; 2, se for considerada média; 3, se for considerada forte ou, finalmente, 4, caso seja considerada potencial.

A terceira etapa, por sua vez, significa apontar as variáveis fundamentais para o desenvolvimento do sistema, podendo ser realizada, inicialmente, mediante classificação direta; em seguida através de uma classificação indireta, denominada Matriz de Impactos Cruzados - Multiplicações Aplicadas a uma Classificação (MICMAC). Essa classificação indireta acontece quando se eleva à potência da matriz preliminar. (GODET; DURANCE, 2011).

Santos *et al* (2004) mostram que o emprego da técnica na forma de matriz admite que a prospecção de situações futuras falha na apreciação dos diversos impactos quando realizada separadamente. Essa técnica consiste em analisar o futuro a partir de outros eventuais futuros. Dessa maneira, esse estudo matricial é qualitativo e precisa da percepção de especialistas para apontar a possibilidade de ocorrência de um fenômeno.

Outra técnica empregada neste estudo é a relação de força entre atores, seus desafios e objetivos.

O **método da análise dos jogos de atores**, designado por MACTOR (Método de Atores, Objetivos, Relações de força) procura avaliar as relações de força entre atores e estudar as suas convergências e divergências relativamente a um certo número de desafios e de objetivos associados. (GODET; DURANCE, 2011, p. 69, grifo nosso).

Para esses autores, o método MACTOR é composto por sete fases, conforme descrição a seguir:

- **A construção do quadro das estratégias dos atores**, que se refere aos atores que controlam as variáveis-chave, em que as informações são

agrupadas segundo suas identidades (finalidades, objetivos, projetos e motivações) e seus meios de ação;

- **A avaliação das relações de força entre os atores**, em que é elaborada uma matriz das influências diretas entre os atores, utilizando o quadro da primeira fase e considerando os mecanismos de ação de cada ator. Nessa fase, ocorre a análise da relação entre os atores, conforme o grau de influência: o ator tem pouca influência ou nenhuma sobre outro ator (0); o ator tem influência sobre os processos de gestão do outro ator (1); o ator tem influência sobre os projetos do outro ator (2); o ator tem influência sobre a missão do outro ator (3); e o ator tem influência sobre a existência do outro ator (4). Essa avaliação destaca as forças e as vulnerabilidades de cada ator, categorizando-os em: atores dominantes (muito influentes e pouco dependentes); dominados (pouco influentes e muito dependentes); de ligação (tão influentes quanto dependentes); e os autônomos (nem influentes nem dependentes);
- **Identificação dos desafios estratégicos e dos objetivos associados, que podem ser consonantes ou diferentes;**
- **Posicionamento dos atores em relação aos objetivos e identificação das semelhanças e diferenças**, que se refere a uma descrição (por meio de uma matriz atores x objetivos) da posição de cada ator sobre o objetivo podendo indicar o seu acordo (+1), o seu desacordo (-1) ou a sua neutralidade (0);
- **Hierarquização das preferências no que se refere aos objetivos de cada ator**, em que se analisa a intensidade da posição de cada ator mediante uma escala especial;
- **Integração das relações de força na análise das consonâncias e oposições entre atores**, que busca adequar as relações de forças de cada ator à intensidade de sua posição acerca dos objetivos, possibilitando visualizar a deformidade das alianças e conflitos potenciais;
- **Elaboração das propostas estratégicas e das questões-chave para o futuro.**

Outra técnica utilizada neste estudo é a análise morfológica, que consiste na construção dos cenários possíveis.

Essa técnica compreende o desenvolvimento e o uso prático de

procedimentos basilares, que proporcionem encontrar e analisar as relações estruturais de objetos ou fenômenos para que possa construir realidades aceitáveis. (SANTOS et al, 2004).

A **análise morfológica** visa explorar de forma sistemática os futuros possíveis a partir do estudo de todas as combinações resultantes da decomposição de um dado sistema. Este método é hoje utilizado principalmente na construção de cenários. Pode igualmente permitir pôr em evidência processos ou produtos novos em matéria de previsão tecnológica. (GODET; DURANCE, 2011, p. 74, grifo nosso).

Essa ferramenta possui duas etapas. Inicialmente, decompõe-se o sistema em subsistemas ou elementos, que devem ser autônomos e abarcar a integralidade do sistema analisado. Dessa maneira, os cenários são produtos da reunião das várias configurações individuais que são determinadas em cada um dos elementos, que formam o sistema total. Nesse sentido, a quantidade de possíveis cenários depende de quantas combinações de hipóteses são possíveis construir. O segundo momento dessa análise reduz o espaço morfológico preliminar a um subespaço utilizável, por meio da inserção de parâmetros de exclusão e de escolha, baseando-se em combinações convenientes, que poderão ser apreciadas. Além disso, é possível inserir uma etapa acessória, denominada cenários em caixas, que são necessários para a análise minuciosa de sistemas muito complexos, construindo dois tipos de cenários: parciais e globais. Os cenários parciais podem ser agrupados para formar os cenários globais. (GODET; DURANCE, 2011).

Além desses instrumentos, este estudo será complementado pela técnica de **análise de conteúdo**, usada na avaliação de materiais sobre ciber terrorismo, que foram levantados na aplicação do formulário, bem como textos e notícias, referente ao terrorismo cibernético, que foram divulgados nos *sites* das organizações estudadas.

A Análise de Conteúdo é uma técnica para se estudar e analisar a comunicação de maneira objetiva, sistemática e quantitativa. Buscam-se inferências confiáveis de dados e informações com respeito a determinado contexto, a partir dos discursos escritos ou orais de seus atores. A Análise de Conteúdo pode ser aplicada virtualmente a qualquer forma de comunicação: programas de televisão, rádio, artigos da imprensa, livros, poemas, conversas, discursos, cartas, regulamentos etc. (MARTINS, 2008, p. 33).

Michel (2009) afirma que a análise de conteúdo é um instrumento de exame de dados, em que a análise acontece depois do levantamento. Esta técnica utiliza textos, falas e informações, que foram coletados de maneira prévia.

Então, este capítulo realça o caminho a ser percorrido neste estudo, destacando a sua natureza prospectiva, empregando, sobretudo, o método e as técnicas, que foram propostos por Godet para a coleta, a análise e a descrição dos resultados, que serão apresentadas no quarto capítulo, depois da revisão de literatura, que constituirá o próximo capítulo, em que abordará a Gestão da Segurança da Informação e o Ciber terrorismo ou Terrorismo Cibernético.

3 REVISÃO DA LITERATURA

Esta revisão de literatura aborda tópicos sobre a Gestão da Segurança da Informação (GSI) e a respeito do Ciber terrorismo, apresentando conceitos e exemplos, que irão subsidiar as análises deste estudo. Dessa forma, este capítulo é composto por duas seções. A primeira trata da GSI, destaca os conceitos de informação, ativo informacional, ameaça, vulnerabilidade, risco, segurança da informação e princípios básicos. A segunda expõe o ciber terrorismo, mostrando nesta ordem: o terrorismo; o ciberespaço; o ciber ativismo; o ciber terrorismo propriamente dito; e os tipos e exemplos de ataques ciber terroristas no Brasil. Tais elementos são relevantes para a composição das definições e exemplificação do ciber terrorismo.

3.1 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

No século XXI, as organizações públicas ou privadas utilizam em demasia a tecnologia da informação e da comunicação, pois este se tornou parte indispensável para realização das atividades do dia-a-dia destas organizações. Da mesma forma, a informação passou a ser considerada um bem de valor patrimonial, ou seja, é um ativo para as organizações. Dessa maneira, a evolução das tecnologias da informação e da comunicação propiciou uma maior eficiência e celeridade no processamento e no trato da informação.

A tecnologia, nesse contexto, é definida como os recursos de *hardware* e *software* que apoiam a tomada de decisão e o gerenciamento de informações e conhecimentos, considerando os indivíduos que participam ativamente desses processos. (ANGELONI, 2008, p. 243).

Percebe-se que as tecnologias da informação e da comunicação são utilizadas no suporte à gestão da informação das organizações, promovendo um maior compartilhamento de informações entre os seus colaboradores.

A informação é um componente intrínseco de quase tudo que uma organização faz. Sem uma clara compreensão dos processos organizacionais e humanos pelos quais a informação se transforma

em percepção, conhecimento e ação, as empresas não são capazes de perceber a importância de suas fontes e tecnologias de informação. (CHOO, 2003, p. 27).

Hong *et al* (2003) definem a informação como um relevante e valioso ativo empresarial, que deve ser protegido de forma correta. Já a NBR ISO/IEC 27002:2005 compreende a informação como um ativo fundamental para os negócios de uma instituição.

[...] precisamos nos lembrar de que a informação é um bem, tem valor para a empresa e deve ser protegida. A informação deve ser cuidada por meio de políticas e regras, da mesma maneira que os recursos financeiro e material são tratados dentro da empresa. Com isso queremos dizer que a informação é um ativo de valor. É um recurso crítico para a realização do negócio e a execução da missão da organização. Portanto, sua utilização deve ter regras e procedimentos. (FONTES, 2006, p. 2).

A informação pode ser entendida, de acordo com o inciso I do artigo 4º da lei nº 12.527/2011, como “[...] dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.”

Nota-se que a informação adquiriu o status de bem organizacional. Todavia, não é algo recente, sendo produto de uma discussão que perdura muitas décadas. Ao longo dos anos, ela foi evoluindo, chegando ao patamar de bem intangível.

Os bens organizacionais podem ser classificados como tangíveis, que são os bens físicos ou financeiros, e os intangíveis, que se dividem em intangíveis que geram valor (marcas, inovação e o capital intelectual) e os que protegem valor (Segurança da Informação, Gestão de Riscos e a Governança Corporativa). (FONTES, 2012).

Esta seção discorre sobre a Gestão da Segurança da Informação. Contudo, sentiu-se a necessidade de ilustrar o desenvolvimento da definição do termo informação além de conceitos de elementos relevantes para este estudo.

A informação pode ser compreendida mediante três perspectivas distintas. A primeira definição é mais limitada e está ligada a uma dimensão material, física, sendo estudada sob uma ótica quantitativa e positivista, ou seja, a partir de um modelo sintático de estudo. A segunda concepção é mais ampla e vinculada a uma dimensão cognitiva, em que ocorre a interação entre dados, que é material, e

conhecimento, que está na mente dos indivíduos, sendo estudada a identificação de significados e interpretações, isto é, através de um modelo semântico. A terceira compreensão, que apresenta uma natureza contemporânea, insere a informação no escopo da ação do homem e no cenário de contextos socioculturais concretos, sendo estudada mediante um modelo pragmático. (ARAÚJO, 2014).

Percebe-se que Araújo (2014) apresenta uma evolução relevante na definição da informação, mostrando o seu caráter polissêmico. Todavia, o terceiro conceito é predominante devido a sua praticidade e relevância no âmbito das organizações. Nota-se também que esses diversos sentidos se complementam, contribuindo para a construção de conhecimento e se tornando um bem empresarial.

A informação recebe a denominação de ativo, devido a sua vinculação à área financeira e por ser considerada um elemento de valor tanto para os indivíduos quanto para as organizações. (SÊMOLA, 2014).

O ativo de informação é todo componente de processos que manipulam e processam a informação, sendo categorizado em: informação; tecnologia (equipamentos utilizados); pessoas; processos (sequência de atividades); e o ambiente (local de armazenamento). (MANOEL, 2014).

Nessa perspectiva, este estudo segue o entendimento de informação como um ativo ou um bem fundamental para as organizações, tendo em vista sua permanência no mercado atual, possibilitando uma fonte relevante de vantagem competitiva. Dessa maneira, a informação pode ser considerada matéria prima para o alcance do conhecimento. Além disso, esta pesquisa visualiza uma estreita relação entre a informação e as tecnologias da informação e da comunicação.

Assim, “considerar a informação um bem não é uma invenção da Era da Informação e do Conhecimento, mas são as tecnologias da informação que estão revolucionando a noção de valor que se adicionou à informação.” (ZANON, 2014, p. 71).

Essa relação entre as tecnologias e a informação não apresenta somente uma natureza positiva, porque, com a evolução e a inovação das tecnologias digitais, desenvolveram-se também as ferramentas e as formas de atacar os sistemas de informação das organizações, objetivando sobretudo alterar, modificar suas informações e causar graves prejuízos financeiros para a organização.

Com a disseminação da internet e a evolução das tecnologias da informação e comunicação, as organizações passaram a utilizar, gradativamente, a rede

mundial de computadores como meio essencial para constituição de negócios, aumentando também a probabilidade de incidentes de segurança no ciclo vital da informação: criação, manuseio, armazenamento, transporte e descarte, comprometendo os produtos organizacionais. (SILVA; ARAÚJO; AZEVEDO, 2013).

Isso é possível, porque os sistemas possuem riscos e vulnerabilidades, estando, pois, expostos às ameaças inseridas na grande rede de interconexão mundial, que utilizam as tecnologias para executarem seus ataques.

O reconhecimento preliminar das possíveis ameaças inerentes aos conteúdos digitais trazem benefícios às instituições no tocante à administração de recursos financeiros essenciais para a instalação e manutenção de sistemas e processos operacionais. Identificar esses perigos antecipadamente ou possuir o conhecimento necessário para saná-los ou amenizá-los contribui para a gestão eficiente da informação digital. (BELARMINO; ARAÚJO, 2014, p. 6).

As ameaças são agentes ou situações que provocam incidentes (fatos ou eventos), que comprometem o ativo informacional mediante a exploração de vulnerabilidades, causando perdas de confidencialidade, integridade e disponibilidade, e, por conseguinte, gerando impactos nos processos de negócio de uma organização. (SÊMOLA, 2014).

Sêmola (2014) apresenta uma classificação de ameaças, agrupando-as segundo critérios de intencionalidade. Sobre isso, apresenta-se o quadro 2 na sequência.

Quadro 2 - Classificação de ameaças em grupos segundo sua intencionalidade

Grupos de ameaças	Especificação
Naturais	“Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.”
Involuntárias	“Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.”
Voluntárias	“Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.”

Fonte: Adaptado de Sêmola (2014).

Convém, também, definir aqui as vulnerabilidades. Elas podem ser compreendidas como um conjunto de condições que podem deixar um sistema aberto para invasão, para acesso não autorizado, sistemas indisponíveis, entre outras situações. (SINGH *et al*, 2011).

Singh *et al* (2011, p. 572, tradução nossa) afirmam que

a avaliação da vulnerabilidade em uma comunicação busca identificar fraquezas e vulnerabilidades no sistema, design, implementação ou operação e gerenciamento que poderia ser explorado para violar a segurança do sistema. O escopo geral da avaliação da vulnerabilidade é melhorar a segurança das informações e dos sistemas, avaliando os riscos associados. A avaliação da vulnerabilidade irá definir as diretrizes para parar ou mitigar qualquer risco.

Nessa perspectiva, as vulnerabilidades são fragilidades presentes ou ligadas a ativos informacionais, ou seja, são elementos passivos que só causam um incidente de segurança quando são exploradas por ameaças, prejudicando de maneira negativa um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. (SÊMOLA, 2014).

Sêmola (2014) também apresenta uma série de vulnerabilidades, que existem no contexto organizacional. Acerca disso, destaca-se o quadro 3 a seguir.

Quadro 3 - Exemplos de vulnerabilidades

Vulnerabilidades	Especificação
Físicas	“Instalações prediais que não atendem as boas práticas ou as normas e regulamentações vigentes; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em ambientes com ativos ou informações estratégicos; controle de acesso deficiente em locais contendo informações confidenciais ou sensíveis etc.”
Naturais	“Ambientes com equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura etc.”
Hardware	“Computadores são suscetíveis a poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados, com falhas ou flutuações no suprimento energético ou aumento excessivo na temperatura ambiente.”

Software	“Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações, perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário.”
Mídias	“Discos, fitas, relatórios e impressos podem ser perdidos ou danificados; falhas de energia podem causar panes em equipamentos, podendo danificar trilhas lógicas de dados; discos rígidos usualmente têm vida útil; a radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.”
Comunicação	“A comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.”
Humanas	“Falta de treinamento ou de conscientização das pessoas, falta de avaliação psicológica adequada ou de verificação de antecedentes (<i>background check</i>) que identifique objetivos escusos ou problemas anteriores, ou mesmo má-fé ou o descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou a erros, omissões etc. que ponham em risco as informações.”

Fonte: Adaptado de Sêmola (2014).

Além disso, as vulnerabilidades consideradas mais expressivas para a prevenção da informação digital são a falta de gestão dos ativos informacionais, a omissão de produção de regras e manuais planejados; a ausência de políticas de seleção para a conservação da coleção digital e a inexistência de um controle estatístico com parâmetros importantes para o planejamento, avaliação e gerenciamento do conteúdo arquivado. (BELARMINO; ARAÚJO, 2014).

Em relação à definição de riscos, Ferreira e Araújo (2008) compreendem que se trata de um eventual fato ou ação, que explora vulnerabilidades, causando impactos negativos quando executado.

De outro modo, o risco, no que lhe concerne, é a possibilidade de ameaças explorarem vulnerabilidades, causando perdas dos princípios da segurança da informação e, eventualmente, ocasionando efeitos nos negócios empresariais. (SÊMOLA, 2014).

Nesse contexto, as empresas notaram que suas gestões devem incorporar a segurança da informação, tendo em vista a urgência e necessidade de tratar e

processar as informações de forma segura, adicionando valor ao negócio e minimizando os riscos, as ameaças e as vulnerabilidades.

A Segurança da Informação - SI, conforme o inciso II do artigo 2º do decreto nº 3.505/2000, pode ser compreendida como:

proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000, p. 1).

Essa compreensão tenta abordar a segurança da informação em toda a organização, porque trata da segurança dos sistemas de informação, dos recursos humanos, da documentação e das instalações computacionais.

Hong *et al* (2003) definem a segurança da informação como a utilização de métodos, técnicas e processos gerenciais sobre as informações e os recursos (*hardware*, *software* e dados), para que os ativos organizacionais e a privacidade pessoal mantenham-se protegidos.

A Associação Brasileira de Normas Técnicas também se preocupa com a segurança da informação, definindo-a como:

[...] a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (NBR ISO/IEC 27002:2005, p. 10).

Nota-se que a compreensão de Hong *et al* (2003) e a definição de segurança da informação da NBR ISO/IEC 27002:2005 apresentam uma confluência no sentido de concordar com a ideia de informação como um ativo ou um bem de uma organização. Isso também é base para o entendimento de Fontes (2006).

Segurança da informação 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. (FONTES, 2006, p. 11).

Fontes (2006) afirma também que esse objetivo de proteção da informação consiste em assegurar a sua disponibilidade (deve estar acessível), integridade

(deve estar correta e não alterada), confidencialidade (deve ser acessada e utilizada unicamente pelos que precisam dela e com prévia autorização), legalidade (deve estar conforme as leis), auditabilidade (o acesso e uso devem ser registrados) e o não repúdio de autoria (o usuário não pode negar que criou ou modificou a informação).

Observa-se que Fontes (2006) vincula a segurança da informação à proteção do negócio e objetivos das organizações, destacando a sua função de minimização de riscos. Além disso, ele apresenta alguns elementos relevantes para a SI como: disponibilidade; integridade; confidencialidade; legalidade; auditabilidade; e não repúdio de autoria.

Nessa perspectiva, para o Tribunal de Contas da União (2012), a integridade de informações expressa à veracidade e confiabilidade das informações transmitidas pelo emissor e as recebidas pelo destinatário, ou seja, significa que a informação não foi alterada, modificada, excluída ou violada durante a transmissão do emissor para o receptor. A confidencialidade significa que só pessoas autorizadas possuem o acesso às informações armazenadas ou transmitidas através da rede. A autenticidade assegura a veracidade da origem das informações. A disponibilidade, por sua vez, garante a acessibilidade da informação para as pessoas autorizadas sempre que for solicitada, assegurando a continuidade da prestação do serviço.

Manoel (2014) corrobora com as definições anteriores, apontando os princípios básicos da SI. Sobre isso, evidencia-se o quadro 4, que segue.

Quadro 4 - Princípios essenciais da segurança da informação

Princípios	Descrição
Confidencialidade	“toda informação deve ser protegida de acordo com o grau de sigilo. [...]. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito terão direito de acessá-la.”
Integridade	“característica da informação de manter-se na mesma condição em que foi disponibilizada pelo seu proprietário. [...]. A preservação da integridade envolve proteger as informações contra alterações em seu estado original.”
Disponibilidade	“qualidade de tornar disponível para usuários, sempre que necessário e para qualquer finalidade, a informação gerada ou adquirida por um indivíduo ou organização. Uma informação disponível é a que pode ser acessada por

	aqueles que dela necessitam, no momento em que necessitam.”
Autenticidade	“garantia de que as entidades identificadas em um processo de comunicação, como remetentes ou autores, sejam exatamente o que dizem ser, e de que a mensagem ou informação não tenha sido alterada após o seu envio e recebimento.”
Legalidade	“a informação gerada deve estar em conformidade com leis, regulamentos e contratos. Além disso, a utilização da Tecnologia de Informação e Comunicação deve estar de acordo com as leis vigentes do local ou país.”

Fonte: Adaptado de Manoel (2014, p. 3-4).

Nesse contexto, chega-se na compreensão de Segurança da Informação como um campo do conhecimento voltado para a proteção do ativo informacional contra acessos não permitidos, modificações inadequadas ou sua indisponibilidade. Ou melhor, protege o ciclo de vida da informação (manuseio, armazenamento, transporte e descarte) dos riscos que afetam os três princípios essenciais da segurança da informação: confidencialidade (restrição de acesso e uso somente para pessoas designadas); integridade (manutenção da condição da informação, que foi disponibilizada pelo seu proprietário); e a disponibilidade (a informação deve estar disponível para seus usuários no momento em que eles precisam). Dessa maneira, a segurança da informação possibilita a identificação e o monitoramento de ameaças e vulnerabilidades. (SÊMOLA, 2014).

Kim (2014), por sua vez, recomenda conscientizar as pessoas acerca da segurança da informação, tendo em vista que somente a utilização das tecnologias não assegura a segurança dos sistemas de informação.

Em geral, a SI é entendida pela garantia de seus quatro aspectos fundamentais: a **confidencialidade** – a propriedade de a informação ser acessada por quem estiver autorizado e não ser acessada por aqueles que não possuem autorização; a **integridade** – a propriedade de a informação não ter sido alterada por qualquer agente desautorizado; a **disponibilidade** – o aspecto da segurança que garante que a informação estará disponível para todos os autorizados e que precisem dela sempre que necessário; a **autenticidade** – a propriedade do autorizado ser autêntico, ser aquele mesmo ente autorizado previamente. (FERNANDES; SOUZA, 2016, p. 69, grifo nosso).

Diante desses entendimentos, percebe-se que a segurança da informação deve assegurar, sobretudo, estes princípios fundamentais: confidencialidade;

integridade; disponibilidade; entre outros, que foram apontados nessas definições. Esses três elementos constam em todos os conceitos de SI deste estudo, em que apresentam a mesma essência.

Nessa perspectiva, esta pesquisa partilha dessa compreensão de segurança de informação. Além disso, vai ao encontro das sugestões de Kim (2014), tendo em vista que é necessária a utilização das tecnologias da informação e da comunicação de maneira adequada pelas pessoas, para que haja uma garantia de segurança da informação.

É notório que a segurança da informação é uma condição relevante para o alcance dos objetivos organizacionais. Além do mais, a política de segurança é outro elemento importante nesse contexto organizacional.

A Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação. (FERREIRA; ARAÚJO, 2008, p. 36).

As políticas possuem um papel primordial e uma grande amplitude na organização, podendo ser dividida em três grupos: diretrizes (está no nível estratégico); normas (está no nível tático) e os procedimentos e instruções (está no nível operacional). (FERREIRA; ARAÚJO, 2008).

A política determina a diretriz e a orientação essencial para a segurança da informação de uma organização, mostrando a sua ideologia para a utilização da informação pelos seus funcionários, estagiários, acionistas e diretores. Ou seja, as regras determinadas existem para todos os indivíduos da organização, em que qualquer tratamento diferenciado para usuários deve constar na política de segurança. Nesse sentido, as organizações precisam criar e implantar políticas de segurança para preservar a SI de uma maneira adequada. (FONTES, 2012).

Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (BRASIL, 2012, p. 10).

Além disso, há algumas etapas para a realização de uma política de segurança da informação, como: apreciação de riscos; análise do custo/benefício da

informação; criação de diretrizes e sua normalização em políticas e sua divulgação; pesquisa contínua para atualização da política; programa de treinamento e conscientização dos usuários; e plano de gestão de incidentes. (SILVA; ARAÚJO; AZEVEDO, 2013).

Verifica-se que a elaboração de uma política de segurança da informação é fundamental, pois se trata de um documento que irá mostrar as diretrizes, as normas, os princípios, as sanções que norteiam a segurança da informação de uma organização; podendo ser compreendida como uma política estratégica de uma empresa, pois é essencial para a manutenção e continuidade do seu negócio, permitindo o alcance de suas metas e de seus objetivos organizacionais.

Contudo, no contexto organizacional, percebe-se que só a construção da política não é suficiente para garantir a segurança da informação, mas também são necessários e fundamentais o treinamento e a conscientização dos usuários das tecnologias da informação e dos sistemas de informação.

Do mesmo modo, o sucesso da segurança da informação como uma política estratégica para o alcance dos objetivos da organização está vinculado à Gestão da Segurança da Informação - GSI. Ou melhor, são necessárias as práticas gerenciais nessa área de conhecimento para garantir a proteção do ativo informacional.

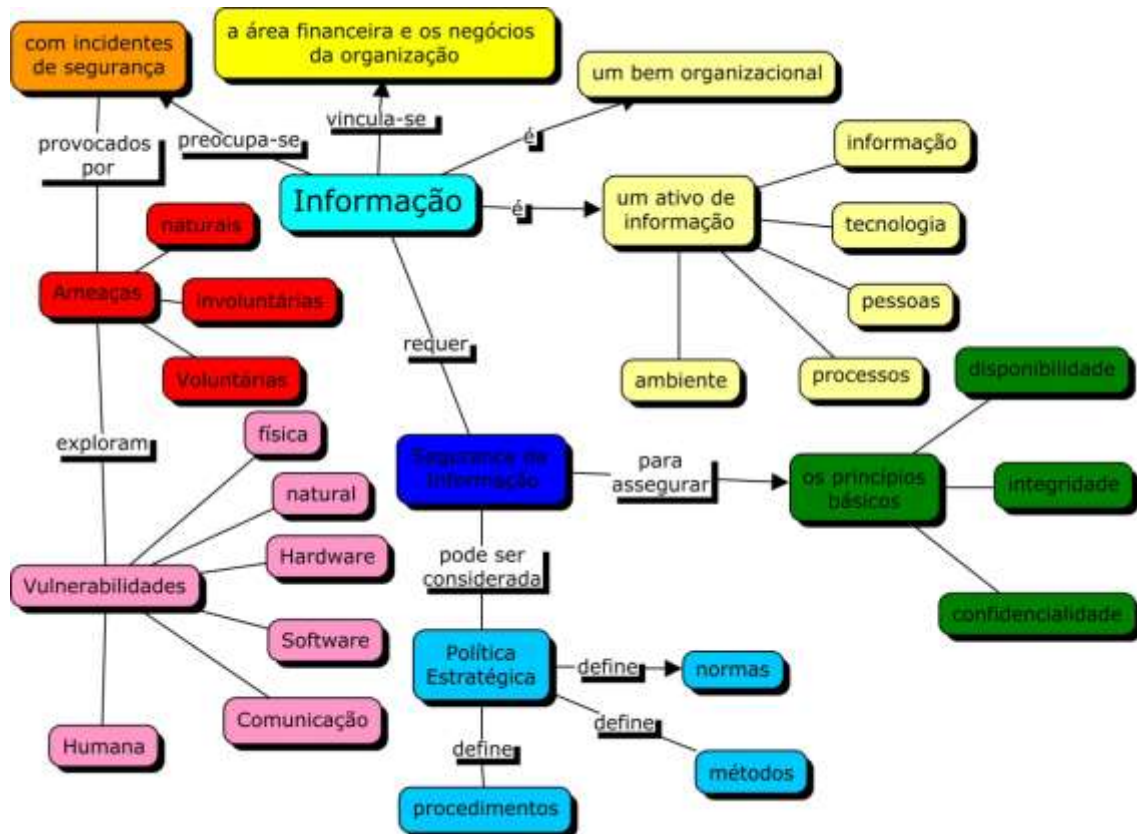
“A gestão da Segurança da Informação tem por objetivo o planejamento, a execução e a monitoração das atividades de SI, e a aplicação de processos de melhoria contínua.” (MANOEL, 2014, p. 57).

A gestão de SI é essencial em uma organização e é de responsabilidade do Chefe de Segurança da Informação, que a executa mediante a metodologia do ciclo PDCA, em que há o *Plan* (planejar), o *Do* (fazer), o *Check* (checar) e o *Act* (agir). Esse ciclo passou por uma evolução e foi adaptado para o ciclo PDCL. Ou seja, a última fase foi substituída pelo *Learn* (aprender). Contudo, tanto o agir quanto o aprender são utilizados na metodologia de GSI. (MANOEL, 2014).

“O ciclo da metodologia de gestão de Segurança da Informação será adaptado para ser utilizado o ‘A’, de *act*, e o ‘L’, de *learn*, em conjunto - assim, os benefícios de cada um são usufruídos de forma harmonizada.” (MANOEL, 2014, p. 60).

Nessa perspectiva, mostra-se a seguir a figura 2, que ilustra e resume as propostas centrais desta seção.

Figura 2 - Mapa conceitual da síntese das ideias centras deste capítulo.



Fonte: Elaborada pelo autor (2017).

Assim, a segurança da informação é justificada no contexto organizacional, tendo em vista que as organizações tratam e processam informações por meio de tecnologias de informação e comunicação, que apresentam vulnerabilidades e estão expostas a vários riscos e ameaças. Nesse cenário, constata-se que as tecnologias evoluem constantemente. Da mesma forma, ocorrem o desenvolvimento e o advento de novos incidentes de segurança da informação, prejudicando a confidencialidade, integridade e disponibilidade do ativo de informação, como exemplo, o ciber terrorismo, que será assunto da próxima seção.

3.2 CIBER TERRORISMO

Vivencia-se o contínuo avanço das tecnologias da informação e da comunicação, propiciando a evolução da tramitação e processamento da informação, que passou a ser considerada um bem de enorme valor para as organizações, ligando-se a área financeira e a manutenção de seus negócios. Esse contexto requer práticas de gestão no campo da Segurança da Informação, como abordado na seção anterior.

Da mesma forma, nota-se o ininterrupto desenvolvimento de outros elementos desta época, convergindo para a utilização das tecnologias. Essa adaptação ocorre, por exemplo, com o terrorismo, que assume novas formas. Nessa perspectiva, esta seção discute o ciber terrorismo como uma nova tipologia de terrorismo, apresentado nesta ordem: os conceitos e características do terrorismo; o lugar de sua atuação (ciberespaço); os conceitos de ciber terrorismo; suas diferenças com o ciber ativismo; e os tipos e exemplos de ataques ciber terroristas registrados no Brasil.

3.2.1 Terrorismo: conceitos e aspectos gerais

Entende-se o terrorismo como um evento antigo, que ganhou atenção especial após os atentados de 11 de setembro de 2001 contra os Estados Unidos. Os recentes atentados, em países europeus, como França em 13 de novembro de 2015, Inglaterra em 22 de maio de 2017, e Espanha em 17 de agosto de 2017, demonstram que o fenômeno precisa de um cuidado específico. Nota-se que o terrorismo também é uma palavra polissêmica, tendo em vista que há diversas definições de várias áreas de conhecimento.

O terrorismo pode ser definido como a prática ou a ameaça de violência, objetivando causar o medo para atingir um propósito político, religioso ou ideológico explícito ou implícito. O risco de terrorismo, por sua vez, não é de fácil definição e se associa a termos como: ameaças; ataques; vulnerabilidades e consequências. (AVEN; GUIKEMA, 2015).

Observa-se o seguinte fragmento de uma notícia, que trata de ataques terroristas no ano de 2016:

Um policial e sua mulher foram assassinados na segunda-feira à noite perto de Paris, em uma ação terrorista de um homem com vínculos jihadistas, que afirmou pertencer ao grupo Estado Islâmico (EI). O terrorista foi morto pelas forças de segurança. O presidente francês, François Hollande, classificou nesta terça-feira de “incontestável ação terrorista” os assassinatos, que aconteceram dentro da residência das vítimas. “A França enfrenta uma ameaça terrorista de grande importância”, advertiu o presidente. (VEJA, 2016b).

Esse trecho ilustra e ratifica que o terrorismo tem o intuito de provocar o terror através de ações violentas. Isso acontece por causa de objetivos políticos, religiosos, sociais e ideológicos. Percebe-se que o terrorismo é comumente praticado por meio da ação de grupos terroristas, como exemplo o Estado Islâmico. Mas há o terrorismo, em que os ataques são de natureza individual.

O terrorismo na forma individual ocorre quando indivíduos atuam sozinhos, ou seja, por conta própria, cometendo atos violentos contra pessoas, causando danos significativos. Eles são influenciados por objetivos sociais, políticos, ideológicos ou religiosos. Essa forma de terrorismo dificulta as ações de inibição, pois não há possibilidade de infiltração, de captura de comunicações, e de detecção baseada em redes. (GORDON; SHARAN; FLORESCU, 2015).

Ferreira (2016) afirma que o conceito de terrorismo de órgãos decisórios dos Estados Unidos possui diversas interpretações legais, permitindo várias inferências, múltiplos argumentos e imensas dúvidas.

Alguns autores afirmam que o terrorismo não apresenta padrão, sendo considerado um fato heterogêneo. Isso pode ser constatado por meio da comparação dos determinantes dos seguintes tipos de terrorismo: o de esquerda, que são os incidentes terroristas realizados por anarquistas, comunistas, socialistas, contrários à globalização, entre outros; e o nacionalista-separatista, que são os terroristas que requerem, principalmente, mudança territorial. Nesse sentido, a discriminação étnica, por exemplo, pode ser relevante para a origem do terrorismo nacionalista-separatista, mas não para o início do terrorismo de esquerda. Todavia, também há aspectos comuns, determinando os diferentes tipos de terrorismo, como: condições econômicas desfavoráveis; populações maiores; entre outros. (BROCKHOFF; KRIEGER; MEIERIEKS, 2016).

Asongu e Nwachukwu (2017) mostram que as diversas tipologias de terrorismo podem influenciar as múltiplas formas de governo (política, econômica e

institucional), impactando geralmente de maneira negativa.

A partir dessa compreensão, percebe-se que o terrorismo não é benéfico em nenhuma perspectiva teórica. Todavia, suas consequências podem modificar, por exemplo, a governança política de um país de maneira positiva ou negativa.

Horgan (2017) apresenta uma compreensão da área psicológica sobre o terrorismo, destacando que foram os ataques de 11 de setembro de 2001, que influenciaram os estudos das diversas áreas de conhecimento acerca desse fenômeno. Nesse sentido, a Psicologia entende o terrorismo como o comportamento, que é o seu objeto de estudo. Além disso, o terrorismo é aceito pela Psicologia como um evento dinâmico, em que um mesmo grupo de terrorista pode mudar, gradativamente, de essência.

Nessa esfera de conhecimento, o terrorismo persiste como uma estratégia interessante para uma multiplicidade de atores e grupos, que utilizam a violência como único meio para efetuar o domínio social, político, ideológico e religioso. (HORGAN, 2017).

O terrorismo foi ampliado a partir do avanço das tecnologias da informação e da comunicação, que encurtaram a distância entre as nações, tornando-se ameaças para a segurança. (ALAIMO; TONG, 2017).

Assim, a partir dessas compreensões, este estudo aceita a definição de que o terrorismo é a ação violenta de indivíduos ou grupos, causando o medo ou terror para alcançar um projeto político, social, religioso ou ideológico. Além disso, entende que esse fenômeno evoluiu, adequando-se ao desenvolvimento das tecnologias digitais. Isso acontece sobretudo por meio de uma nova modalidade de terrorismo: o ciber terrorismo, que é a terminologia mais apropriada nesse contexto, tendo em vista que se constitui em uma versão de terrorismo que utiliza as tecnologias para executar seus ataques. Essa tipologia de terrorismo será destacada mais adiante. Antes, discute-se o seu espaço de atuação: o ciberespaço.

3.2.2 Ciberespaço

A partir do surgimento das tecnologias da informação e comunicação, que são produtos da ação humana, notam-se alguns impactos sobre a sociedade, dentre os quais destacam-se as novas formas de comunicação e interação, utilizadas pelas

peças do mundo contemporâneo. Do mesmo modo, surgiu o ciberespaço, que utiliza as tecnologias como suporte essencial, viabilizando outras maneiras de tratar, processar e transmitir a informação. Além disso, esse espaço reduziu o tempo e a distância para o acesso à informação.

“As tecnologias digitais surgiram, então, como a infraestrutura do ciberespaço, novo espaço de comunicação, de sociabilidade, de organização e de transação, mas também novo mercado da informação e do conhecimento.” (LÉVY, 1999, p. 32).

Nesse contexto, nota-se que o computador se tornou o principal apoio do ciberespaço, devido a sua capacidade de produzir e tramitar a informação por meio de uma rede de computadores.

O computador não é mais um centro, e sim um nó, um terminal, um componente da rede universal calculante. Suas funções pulverizadas infiltram cada elemento do tecnocosmos. No limite, há apenas um único computador, mas é impossível traçar seus limites, definir seu contorno. É um computador cujo centro está em toda parte e a circunferência em lugar algum, um computador hipertextual, disperso, vivo, fervilhante, inacabado: o ciberespaço em si. (LÉVY, 1999, p. 44).

Nessa perspectiva, Lévy (1999) define o ciberespaço ou a virtualização da comunicação “[...] como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. (LÉVY, 1999, p. 92).

O ciberespaço foi possivelmente o sistema de comunicação que mais rápido se generalizou em nível mundial. (LÉVY, 2003).

O ciberespaço é uma virtualização, a atualização em um lugar, de dados registrados em outro lugar, interconectados por redes, e que, por suas características técnicas de programação, permite a mediação da comunicação entre seres humanos, e com a própria cultura por eles produzida, principalmente, se considerarmos que os dados que aparecem na tela do meu computador em um site podem estar hospedados em um lugar físico do outro lado do mundo. (SOUZA; COSTA, 2005, p. 108).

Moraes (2011) afirma que o ciberespaço está caracterizado como um espaço móvel, de criação, aberto a figuras, cores, sons, linguagens e signos.

Percebe-se que essas compreensões convergem no sentido de que o ciberespaço é um espaço virtual de comunicação, que utiliza, sobretudo, o computador e a rede de interconexão mundial como suportes para efetuar a interação entre seres humanos. O entendimento de Moraes (2011), por sua vez,

complementa a definição de ciberespaço de Lévy, Souza e Costa, pois insere alguns elementos importantes, como espaço móvel e de criação, nesse contexto.

[...] o ciberespaço é um espaço semântico/semiótico, onde o signo se dá em várias semióticas, desterritorializado, nômade, em escrita espacializada e com a memória em constante modificação. Se a *Internet* é a rede mundial de computadores, base técnica do ciberespaço, este é a rede de signos e pessoas. (MONTEIRO; FIDENCIO, 2013, p.38).

Nesse cenário, Boff e Fortes (2014) apresentam uma compreensão de ciberespaço como um espaço virtual e social, constituído pelo fluxo de informações e de mensagens disseminadas entre computadores, sendo considerado uma rede aberta, em que qualquer pessoa pode ter acesso. Além disso, esse espaço dispõe de um viés interativo, viabilizando aos usuários a criação de dados e a navegação.

Verifica-se que o ciberespaço está vinculado à diversas áreas de conhecimento, possibilitando a realização de múltiplas atividades. Pode-se dizer que é uma terminologia contemporânea para espaço virtual. “O espaço virtual é comumente chamado de ciberespaço, mundo virtual, realidade virtual, entre outras denominações.” (AZEVEDO, 2014, p. 53). Além disso, percebe-se que esse espaço é aberto para o acesso de qualquer pessoa. Isso requer que as informações pessoais e comerciais disponíveis no ciberespaço sejam, progressivamente, protegidas. (AZEVEDO, 2014).

No período vigente, o conceito de ciberespaço também é trocado ou entendido algumas vezes como sinônimo de Internet. Todavia, isso não pode acontecer, porque são definições distintas, que estão ligadas. A Internet é a rede mundial de computadores, sendo considerada base material do ciberespaço. (AGUIAR; BRENNAND, 2016).

Nessa perspectiva, essas autoras definem o ciberespaço como:

“[...] um mundo virtual onde são disponibilizados variados meios de comunicação e interação em sociedade, com dados, informações e conhecimentos mixados a imagens, sons, e hipertextos, de durabilidade incerta presentes em tempo real ou não.” (AGUIAR; BRENNAND, 2016, p. 46).

Essa compreensão de ciberespaço parece ser mais completa, tendo em vista que o trata como um espaço virtual onde ocorre a comunicação e interação entre os seres humanos. Isso é um entendimento comum nas definições anteriores. Além

disso, esse conceito engloba dados, informações e conhecimentos, misturando-os a imagens e sons.

Assim, verifica-se que o ciberespaço é o espaço virtual, aberto, móvel, de comunicação que utiliza, sobretudo, o computador, a internet, como tecnologias básicas para processar, armazenar, trocar, transmitir dados, informações e conhecimentos. Essas tecnologias são usadas para a comunicação e interação das pessoas. Todavia, esse espaço não apresenta a informação, totalmente, segura, pois há ataques de terroristas a essas redes, objetivando causar diversos prejuízos. Além disso, o ciberespaço é um espaço aberto para o acesso de qualquer pessoa. Do mesmo modo, as formas de terrorismo evoluíram para acompanhar os avanços das tecnologias e, conseqüentemente, do ciberespaço, que pode ser considerado o local em que acontece uma nova tipologia de terrorismo: o ciber terrorismo.

3.2.3 Terrorismo Cibernético ou ciber terrorismo

O ciber terrorismo ou terrorismo cibernético está vinculado ao surgimento e à evolução das tecnologias da informação e comunicação, principalmente os computadores e a internet; bem como ao ciberespaço, em que o processamento e a troca de informações ocorrem de maneira rápida. Pode ser considerado o lado ilícito desse contexto, visto que a sua finalidade é causar danos e prejuízos para pessoas, empresas, governo. Além disso, pode ser considerado umas das maiores ameaças à segurança da informação na atualidade.

O ciber terrorismo é um evento de difícil definição. Isso impossibilita alcançar uma boa solução para combatê-lo. Dessa maneira, há alguns tipos de ciber terrorismo: o legítimo; terrorismo como teatro; e o novo terrorismo. O primeiro também pode ser chamado de puro ou genuíno e são os ataques praticados contra computadores, redes e informações inseridas nos computadores, ou seja, são as atividades de terrorismo que são executadas integralmente no ciberespaço, em que só o computador é o alvo. O segundo pode ser compreendido como uma metáfora, posto que os incidentes terroristas são simulados através de *sites* próprios dos grupos terroristas. Esses *sites* são utilizados para solicitar dinheiro, divulgar mensagens, promover a sua causa e recrutar novos terroristas. O novo terrorismo, por sua vez, acontece mediante as recentes organizações terroristas que são,

extremamente, financiadas. Além disso, são considerados grupos, tecnologicamente, estruturados, apresentando capacidade de causar danos avassaladores a um amplo conjunto de alvo. Nesse sentido, não é apenas o computador o centro dos ataques, mas também as outras áreas do espaço virtual. (GORDON; FORD, 2002).

O ciber terrorismo legítimo tem predominado, pois o computador é considerado a principal ferramenta dos ciber terroristas ou o principal alvo desses. Nesse sentido, a violência do terrorismo tradicional também ocorre e prevalece na realidade virtual. Nessa perspectiva, os terroristas utilizam o computador para roubo de identidade, inserir vírus, usar *malware*, destruir ou alterar dados e manipular preços de ações. Os ciber terroristas podem, por exemplo, usar a identidade roubada para praticar atos terroristas, utilizando a identificação do computador alvo. (GORDON; FORD, 2002).

Observa-se também que esses autores compreendem que as tecnologias da informática facilitam o recrutamento de novos indivíduos, que compartilham da causa terrorista, dispensando o contato físico entre pessoas. Além do mais, os recursos da informática favorecem os acordos entre grupos terroristas, que partilham dos mesmos ideais políticos, sociais e econômicos. (GORDON; FORD, 2002).

Lázaro (2009) afirma que não há uma definição exclusiva de ciber terrorismo, conceituando o como a forma de terrorismo, em que os terroristas utilizam as tecnologias de informação e de comunicação para provocar o medo, objetivando atingir seus interesses. Ou melhor, é uma atuação ilegal denominada de crime cibernético, que utiliza o computador por meio da Internet como ferramenta principal para produzir o terror contra pessoas físicas, organizações públicas e empresas privadas.

Nessa perspectiva, o ciber terrorismo tornou-se uma ameaça expressiva, tendo em vista que o computador e a internet realizam atividades fundamentais na sociedade vigente, como o registro e o arquivamento de uma grande quantidade de dados ou informações. Isso vincula às tecnologias a sociedade através de uma relação de dependência. Dessa maneira, o ciber terrorismo usa as tecnologias para divulgar conteúdos ilícitos, influenciar e anunciar o terrorismo, conseguir recursos e recrutar pessoas. (LÁZARO, 2009).

Percebe-se que a compreensão de Lázaro (2009) vai ao encontro do entendimento de Gordon e Ford (2002) em relação à dificuldade de definir o ciber

terrorismo. Além disso, esses autores mostram que o computador é a principal ferramenta dessa nova tipologia de terrorismo.

O ciber terrorismo pode ser compreendido como a exploração de equipamentos da rede de computadores para provocar o seu mau funcionamento. Isso também é realizado mediante a utilização de dispositivos móveis, como o telefone celular, que apresentam gradativamente mais recursos tecnológicos. (CHU *et al.*, 2011).

Ahmad e Yunos (2012) também apresentam uma compreensão de que o terrorismo cibernético é a realização de ataques por meio do ciberespaço e do universo virtual. Além disso, esses autores mostram que não existe uma definição de ciber terrorismo totalmente aceita, e que há várias interpretações distintas, desafiando a luta contra essas ameaças.

Nesse contexto, Ahmad *et al.* (2012) afirmam que é relevante perceber as semelhanças e as diferenças acerca do que se constitui o terrorismo cibernético para elaborar políticas para o combate dessa ameaça. Para tanto, é proposto um quadro conceitual do ciber terrorismo, que é composto pelos seguintes elementos: alvo (sistemas de computadores, infraestrutura crítica, população civil); motivação (política, ideológica, social); ferramentas de ataque (ataques via rede, operações psicológicas); domínio (ciberespaço); métodos de ataque (meios ilícitos); e impacto (distúrbios em massa, pânico, mortes, perdas econômicas, interferência em serviços críticos). A figura 3 destaca esses elementos.

Figura 3 - Elementos do Ciber terrorismo



Fonte: Adaptado de Ahmad *et al.* (2012).

Hua e Bapna (2012) definem o terrorismo cibernético como uma atividade

realizada através do computador, rede e internet, objetivando intervir, politicamente, socialmente ou economicamente, no desempenho de um grupo, organização ou país. Além disso, pode causar violência física ou terror. Isso é estimulado pelas ideologias clássicas do terrorismo.

Os ataques de ciber terroristas são diferenciados, pois requerem menos pessoas e materiais. Os seus atos também são anônimos e controlados remotamente, dificultando o rastreamento dos ciber terroristas. Os terroristas cibernéticos podem ainda provocar grandes perdas financeiras e medo por meio de seus ataques. (HUA; BAPNA, 2012).

Hua e Bapna (2013) apresentam uma distinção entre *hackers* comuns e ciber terroristas, afirmando que ambos utilizam as tecnologias da computação para executarem seus ataques, mas o propósito diverge. O primeiro busca acessar e modificar dados e arquivos sem a devida autorização, bem como impossibilita serviços para usuários autorizados. Os ciber terroristas, por sua vez, são indivíduos ou grupos, que executam ataques, objetivando causar terror ou medo. Os ataques do terrorismo cibernético contra infraestrutura ou sistemas de negócios são considerados mais graves. Dessa maneira, o ciber terrorismo pode conduzir a uma enorme perda pecuniária.

O ciber terrorismo também pode ser definido como um crime universal e uma ameaça mundial, exigindo uma resposta transnacional. Nesse sentido, os ciber terroristas utilizam o computador como instrumento para fragmentar outros computadores, causando danos no espaço virtual e no mundo real, como a destruição de bens ou a perda da vida. (TEHRANI; MANAP; TAJI, 2013).

Nesse âmbito, as ações para combater o terrorismo cibernético devem ser internacionais, sendo necessária e relevante uma definição jurídica comum, que seja compartilhada por todos os países. Isso contribui para o processo de investigação, permitindo a colaboração entre os países. Dessa maneira, a cooperação e o esforço conjunto global são os procedimentos mais adequados para lutar contra o ciber terrorismo. (TEHRANI; MANAP; TAJI, 2013).

Harries e Yellowlees (2013), por sua vez, afirmam que provocar dano e causar medo são os objetivos essenciais dos ciber terroristas, realizando suas atividades por meio da Internet. Esses autores mostram que até mesmo o setor de saúde não está protegido dessa ameaça, visto que está, paulatinamente, dependente da Internet para executar suas atividades. Nesse cenário, pode ocorrer

uma série de ataques cibernéticos como: derrubar o sistema de computadores de um hospital; divulgar registros médicos particulares; e alterar dados eletrônicos dos pacientes. Isso compromete o cuidado do paciente e torna o sistema de saúde desconfiável.

Jarvis, Macdonald e Nouri (2014) mostram que há duas perspectivas em relação ao ciber terrorismo. A primeira observa esse evento como uma legítima ameaça à segurança da informação. A segunda não acredita que o ciber terrorismo seja uma ameaça, mas uma criação midiática.

Isso confirma a divergência conceitual em relação ao ciber terrorismo, tendo em vista que não há uma consonância de que esse fenômeno constitui uma ameaça à segurança da informação. Além disso, não existe consenso a respeito dos alvos potenciais dos ciber terroristas. (JARVIS; MACDONALD; NOURI, 2014).

Nessa perspectiva, o ciber terrorismo pode ser os ataques, que utilizam, efetivamente, a internet, contra computadores, que são capazes de causar destruição, mortes, quedas densas de energia, desastres de aeronaves, poluição rigorosa da água e perda de convicção na economia global do setor. (KONTSELIDZE, 2015).

Ayres e Maglaras (2016) compreendem que os ciber terroristas projetam ataques para qualquer lugar do mundo. Isso torna o ataque um ato realmente global. Além disso, os ciber terroristas utilizam equipamentos digitais para realizarem seus ataques, reunindo informações essenciais de seus alvos, as quais estão disponíveis de maneira voluntária na internet.

Esses autores destacam ainda que o alvo do ciber terrorismo pode ser o público em geral, bem como um eventual vírus mimético é considerado um método concreto de ataque, influenciando o comportamento de uma população. (AYRES; MAGLARAS, 2016).

Enfim, verifica-se que existem diversas definições sobre o ciber terrorismo, considerando o elemento a ser destacado: alvo; motivação; ferramentas de ataques; domínio; métodos de ataques; impactos. Essa diversidade dificulta a investigação, o rastreamento e o enfrentamento dos ciber terroristas. Dessa maneira, a perspectiva clássica de terrorismo cibernético predomina na sociedade vigente, em que se utiliza o computador e a internet como ferramenta ou como alvo. Essa nova tipologia de terrorismo possui motivação semelhante ao terrorismo tradicional, que é ideológica, social, política e/ou religiosa. Todavia, o ciber terrorismo é executado no

ciberespaço, atacando computadores, redes e sistemas informáticos. Além disso, ele causa, principalmente, prejuízos monetários, medo e mortes. Constata-se ainda que o terrorismo cibernético é, habitualmente, confundido com o ciber ativismo. Este tema será apresentado na sequência.

3.2.4 Ativismo no ciberespaço ou Ciber ativismo

O ativismo também se adequou à evolução das tecnologias da informação e da comunicação, criando o ciber ativismo, que é uma nova tipologia de ativismo, conexo ao mundo contemporâneo e interconectado. O ciber ativismo, similarmente ao ciber terrorismo, utiliza o computador e a internet como ferramentas essenciais; bem como é executado no ciberespaço.

Alguns pontos diferenciam o ciber terrorismo do ciber ativismo, que é um movimento político que apresenta a liberdade de informação e de comunicação como conteúdos centrais, constituindo-se na referência fundamental dos movimentos de oposição às formas de dominação mediante controle difuso. (NEVES, 2010).

Da mesma forma que, na atualidade, os indivíduos transferiram para a internet suas interações em redes sociais, mantendo-as ou modificando-as, o ativismo em prol de causas socioambientais, que anteriormente se manifestava apenas em ambientes *offline*, passou a se disseminar pela internet e suas redes sociais digitais. Os grupos compostos por indivíduos que defendem melhorias sociais e ecológicas passaram a explorar os ambientes *online* como forma de disseminar seus discursos de pressão política, objetivando atingir de forma viral os mais diversos públicos. (LIMA, 2012, p. 73).

Lima (2012) mostra que o ativismo digital, que também pode ser denominado de ciber ativismo, baseia-se, essencialmente, no reforço das convicções culturais de um grupo definido mediante a utilização das redes sociais digitais (*Twitter, Facebook, Orkut e Youtube*). Para a autora, a internet potencializa as ações de ativismo, em que é possível identificar mensagens sugerindo crítica às leis, defesa de animais, erradicação da violência e convite para eventos, ou seja, várias maneiras de ativismo. “O indivíduo é estimulado a aderir às diversas causas, estabelecendo uma sensação de pertencimento e, em paralelo, de distinção entre os demais.” (LIMA, 2012, p. 74).

O ciber ativismo é inerente às recentes ferramentas tecnológicas, principalmente a internet. Dessa forma, os *sites* de redes sociais se estabelecem como instrumento essencial dos grupos ciber ativistas, considerando sua abrangência e facilidade de utilização. Além disso, essas ferramentas possibilitam aos ciber ativistas uma forma de comunicação horizontal e mais visibilidade na rede e na mídia. (MONTARDO; ARAÚJO, 2013).

O ciber ativismo é o protesto na forma *on-line*, que é executado por meio das tecnologias da informação. Estes protestos são de natureza política, social e religiosa. Essa nova tipologia de ativismo apresenta um processo evolutivo e pode ser classificada em ciber ativismo 1.0 e ciber ativismo 2.0, considerando o avanço das tecnologias. O primeiro se caracteriza pela utilização de ferramentas como o e-mail para divulgar as reivindicações dos ativistas. O segundo estágio de evolução apresenta como atributo o uso pelos grupos ativistas de ferramentas e aplicações de redes sociais como o *youtube*, *twitter*, *facebook*, entre outras, para realizar e organizar seus protestos. Além disso, há outros instrumentos (*whatsApp* e *Skype*) que podem ser empregados na prática do ciber ativismo. (SANDOVAL-ALMAZAN; GIL-GARCIA, 2014).

Percebe-se que o ativismo digital também pode ser executado nos protestos da área ambiental. “Uma das estratégias do movimento ambientalista na Internet é o ciber ativismo com intuito de aprimorar a atuação de grupos, ampliando as técnicas tradicionais de apoio.” (GOMES JR., 2015, p. 567).

O ciber ativismo consiste em assinar petições e enviar cartas já escritas pelas ONGs a presidentes, governadores, parlamentares, ministros ou grandes empresários. Os indivíduos são convocados a participar de campanhas como conexões ou nós em uma rede eletrônica de informações, e, não mais como sujeitos no sentido clássico, que pressupunha autonomia de julgamento, independência, originalidade, personalidade, reflexão. (MARZOCHI, 2015, p. 138).

Nota-se, a partir desses conceitos, que o ciber ativismo é uma forma de protesto político, social e ambiental, que ocorre através da rede eletrônica de informações, em que os computadores e a Internet são as ferramentas fundamentais.

Mota e Figueiredo Filho (2015) mostram o ativismo *hacker* ou *hacktivismo*, que é outra vertente do ativismo digital, que utiliza ferramentas digitais transgressivas e o anonimato para realizar protestos políticos na Internet. Esses

autores analisam a rede *Anonymous* Brasil, que é um exemplo de *hacktivismo* no contexto brasileiro. Essa rede realizou uma sucessão de protestos cibernéticos contra a Copa do Mundo de 2014 mediante o emprego de tecnologias digitais para defender razões sociais, a transparência de Estados e empresas.

Dessa maneira, esses atores executam atividades que, juridicamente, são discutíveis, como, por exemplo, vazar documentos sigilosos de autoridades públicas. Todavia, eles diferem da rede terrorista, tendo em vista que a violência e o lucro monetário não fazem parte de suas motivações. Assim, o *hacktivista* age em prol de fins ideológicos e causas políticas de mudança. (MOTA; FIGUEIREDO FILHO, 2015).

O *hacktivismo* não apresenta intenção criminosa, preocupando-se com eventuais acusações de criminalidade e terrorismo durante o protesto *on-line*. Todavia, não há o reconhecimento do *hacktivismo* como uma prática legítima de ativismo, bem como existe uma tendência de inserir todos os protestos virtuais na relação de ameaças cibernéticas. (VLAVO, 2015).

A mídia tradicional apresenta um entendimento equivocado sobre o *hacker*, definindo-o como um ser criminoso, que persegue senhas de banco e rouba dados. Em realidade, a comunidade *hacktivista* pode infringir leis para realizar atos em prol de um bem maior. Para tanto, o *hacker* utiliza os seguintes princípios motivadores: liberdade de expressão; livre acesso à informação; privacidade; e combate à tortura. (BARRETO JUNIOR; AULER; BARBOSA, 2016).

Em geral, o ciber ativismo é compreendido como o emprego das tecnologias da informação e da comunicação, sobretudo a internet, por movimentos sociais e ativistas. (ALCÂNTARA, 2016).

Por outro lado, podemos apontar o ciber ativismo como uma nova configuração comunicativa dos movimentos sociais, caracterizada pela reestruturação das práticas cotidianas de comunicação, por interações mediadas pelas NTICs e pela conexão digital entre indivíduos, grupos e sociedade. Esse novo padrão comunicativo implica na geração de novas dinâmicas de confronto, temporalidades e espacialidades para a ação coletiva contemporânea, assim como de subjetividades políticas. (ALCÂNTARA, 2016, p. 332).

Então, compreende-se que o ativismo se adequou ao novo cenário mundial, em que se realizam seus protestos por meio das tecnologias da informação e da comunicação, em especial o computador e a internet. Na verdade, foi realizada uma

transformação nas práticas de protestos sociais, políticos e ambientais, originando o ciber ativismo, que também pode ser chamado de ativismo online, ativismo digital, ativismo virtual e ativismo em rede. “As práticas ciber ativistas consistem em reformulações de práticas de ativismo social cuja existência é anterior ao ciberespaço.” (FLORES; GOMES, 2017, p. 223). Além disso, por meio dessas definições, verifica-se que o *hacktivismo* é, comumente, confundido com o terrorismo cibernético, mas são fenômenos distintos, que se diferenciam de acordo com o propósito. O ativismo *hacker* realiza ataques de caráter transgressor por meio das tecnologias no ciberespaço, mas objetivam protestar em defesa de uma causa política, social, ambiental e provocar uma mudança no contexto. O ciber terrorismo, como vimos na seção anterior, tem a intenção de promover ataques violentos, causar mortes e provocar danos financeiros. Na sequência, mostra-se os principais ataques cibernéticos no Brasil, destacando os de viés ciber terrorista.

3.2.5 Tipos de ataques no Brasil

No Brasil, também, é notória uma relação de dependência entre as organizações e as tecnologias da informação e da comunicação, proporcionando ganhos e benefícios significativos. Por outro lado, houve uma potencialização em relação às diversas formas de ataques cibernéticos, sobretudo as de cunho terrorista.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) está encarregado de tratar os incidentes de segurança em computadores que abarcam as redes conectadas à internet brasileira.

Em relação aos ataques mais recorrentes atualmente, pode-se apontar a engenharia social como um dos mais comuns. O CERT.br (2012, p. 115) define a engenharia social como uma:

Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido “conto do vigário” utiliza engenharia social.

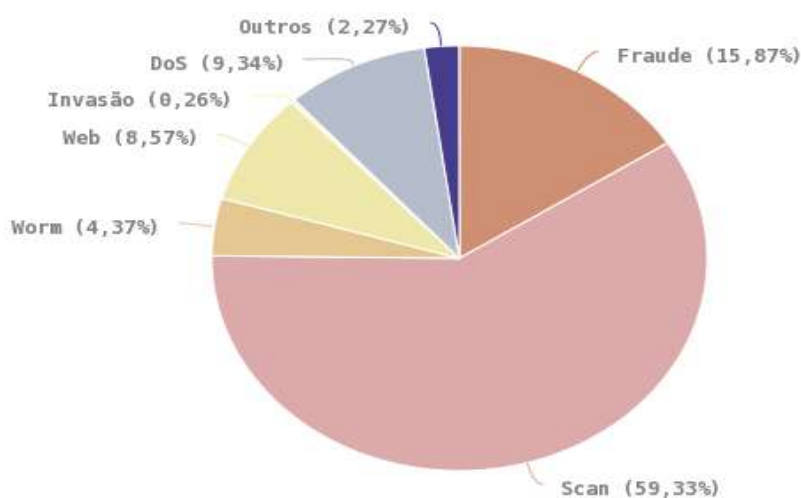
No Brasil, a pesquisa global de segurança da informação de 2014 destaca o comprometimento dos registros de clientes como a principal consequência dos incidentes de segurança, que são causados, sobretudo por *hackers*. Além disso, informa que as organizações estão conscientes de que as ameaças estão aprimoradas, a motivação é diversa e os controles utilizados não são mais capazes de combater os ataques dessas ameaças. (PWC, 2014).

Nessa perspectiva, o CERT.br (2012) mostra que os ataques possuem diversos propósitos e acontecem na internet, direcionado para distintos alvos e utilizando diversas técnicas. Além disso, afirma que qualquer serviço, computador ou rede pode ser alvo de um ataque através da internet. Da mesma forma, qualquer computador pode realizar ataques por meio da internet.

Percebe-se que a pesquisa global de segurança da informação de 2014 corrobora com a proposta da cartilha do CERT.br (2012), na medida em que confirma que há motivações ou propósitos variados para a realização dos ataques cibernéticos.

Na realidade, o CERT.br executa atividades como monitoração, análise, treinamento e conscientização, bem como oferece estatísticas na área de incidentes de segurança, apontando os principais ataques que lhe foram notificados. Em relação aos tipos de ataques, observa-se, por exemplo, o gráfico 2 e o quadro 5 na sequência.

Gráfico 2 - Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2016.



© CERT.br – by Highcharts.com

Fonte: CERT.br (2016).

O quadro 5, que segue, apresenta a descrição dessas tipologias de ataques.

Quadro 5 - Ataques Reportados ao CERT.br

Tipos de ataques	Descrição
worm	“notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.”
dos (DoS -- <i>Denial of Service</i>)	“notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.”
invasão	“um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.”
web	“um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.”
scan	“notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.”
fraude	“segundo Houaiss, é ‘qualquer ato artiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro’. Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.”
outros	“notificações de incidentes que não se enquadram nas categorias anteriores.”

Fonte: Adaptado de CERT.br (2016).

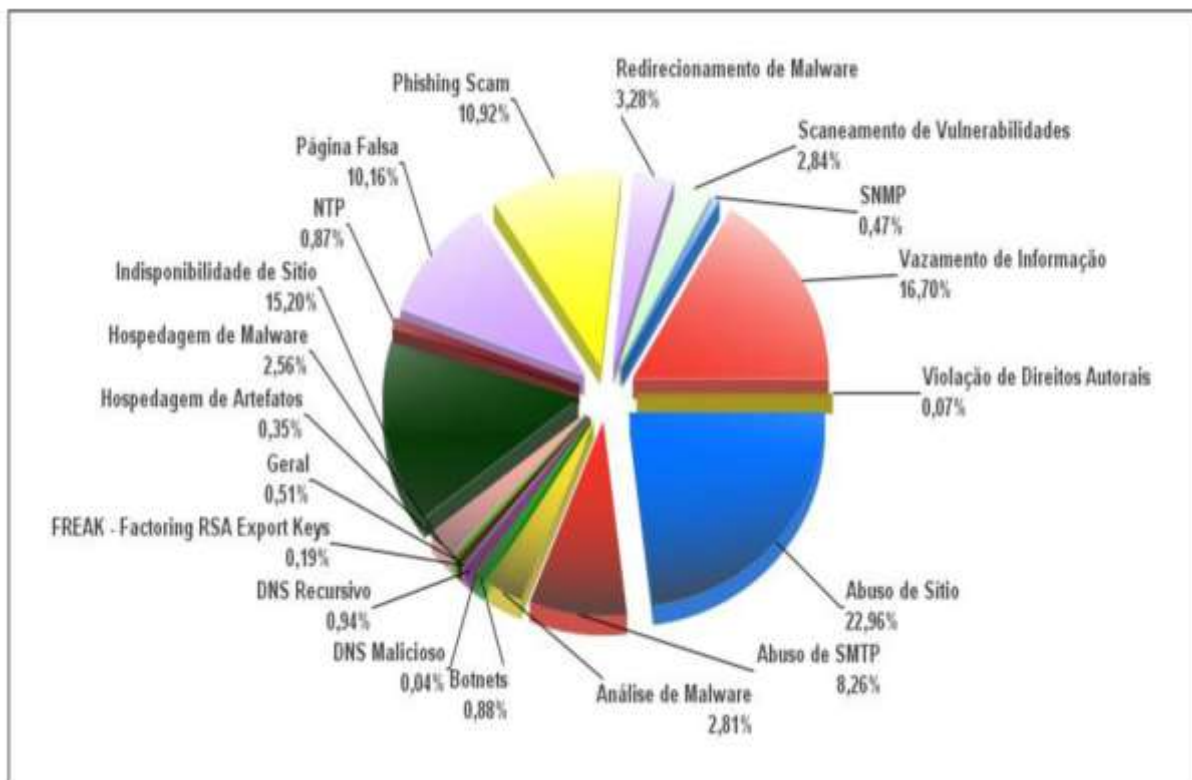
O gráfico 2 e o quadro 5 complementam-se para mostrar os principais incidentes notificados ao CERT.br, em que o gráfico apresenta os percentuais dos ataques e o quadro descreve as referidas ameaças.

Ressalta-se que esses ataques cibernéticos podem estar relacionados ao ativismo digital ou ao terrorismo cibernético. Contudo, o propósito e a motivação do ataque é que pode indicar se o ataque será de ciber ativistas ou de ciber terroristas, ou com outro tipo de motivação, como vimos na seção anterior.

A Administração Pública Federal (APF) também dispõe de um tratamento de incidentes de segurança em redes do governo, que é executado pelo Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da

Administração Pública Federal (CTIR Gov), o qual oferece, estatisticamente, os resultados do trabalho de identificação, análise e resposta aos incidentes de rede de computadores da APF. Observa-se o gráfico 3 abaixo, que exemplifica os principais incidentes reportados ao CTIR Gov em 2016.

Gráfico 3 - Distribuição de incidentes por categoria



Fonte: CTIR Gov (2016).

Nota-se que os incidentes mais reportados ao CTIR Gov no ano de 2016 foram, respectivamente: abuso de sítio (22,96%); vazamento de informação (16,70%); indisponibilidade de sítio (15,20%); *phishing scam* (10,92%); página falsa (10,16%); entre outros. Esse gráfico também mostra que há uma quantidade expressiva de ameaças à segurança da informação da APF, tentando provocar perdas de confidencialidade, integridade e disponibilidade, que necessita de políticas estratégicas da Gestão de Segurança da Informação da APF.

Ressalta-se que esses incidentes podem estar vinculados ao ciber terrorismo, considerando a motivação e o propósito dos ataques. Nessa perspectiva, observa-se a seguir os trechos de uma notícia, que trata e exemplifica um ataque ciber terrorista.

A Divisão Antiterrorismo da Polícia Federal monitorou mensagens trocadas pelos brasileiros em redes sociais, especialmente via

Telegram e Whatsapp, e detectou que havia o risco real de se repetirem no Rio atos extremistas como o que vitimou 50 pessoas na boate Pulse, em Orlando, há pouco mais de um mês. As ordens do grupo virtual “Defensores da Sharia” eram para adquirir armamento, treinar tiro ao alvo e iniciar ou ampliar treinamento em artes marciais [...]

Nas conversas monitoradas com autorização judicial, os suspeitos, que em parte utilizavam nomes fictícios para se identificarem, também discutiam táticas de guerrilha e propagavam intolerância racial, de gênero e religiosa. [...]. Foram interceptadas mensagens de comemoração pelas execuções feitas pelo grupo extremista no Oriente Médio e pelos recentes massacres em Orlando e em Nice.

[...]

O recrutamento do grupo preso nesta quinta-feira foi feito via internet, prática habitual do Estado Islâmico. Não houve contato direto do grupo de brasileiros com terroristas do grupo, embora um dos integrantes da célula no Brasil tenha informado nas mensagens trocadas que estaria disposto a viajar ao exterior para se encontrar com líderes extremistas. (VEJA, 2016a).

Verifica-se que esses fragmentos exemplificam e confirmam os ataques ciber terroristas no Brasil, que utilizam a internet para recrutar novos candidatos, divulgar as ideologias do grupo. É possível visualizar também a utilização de redes sociais para organizar ataques, que provoque violência, medo e mortes.

No primeiro semestre de 2017, tiveram alguns ataques cibernéticos de caráter terrorista de proporção mundial, conforme indicado nos fragmentos que seguem:

O mundo presenciou nesta sexta-feira (12) um ataque hacker em escala global. Mais de 70 países, incluindo o Brasil, foram afetados pelo vírus que sequestra computadores e pede resgate em criptomoedas. Empresas privadas, instituições filantrópicas, hospitais e órgãos governamentais estiveram entre as vítimas e foi comum ao longo do dia registro de organizações pedindo que funcionários desligassem o computador para evitar o ataque. Não se sabe até o momento quem coordenou o ataque e o que será feito para tentar pegar os criminosos.

O ataque se utilizou de um vírus da categoria ransomware conhecido como “WannaCry” (“quer chorar”, em inglês). Ele sequestra os dados do computador infectado e exige um pagamento em criptomoedas, como o Bitcoin, para (supostamente) liberar os dados. Algumas telas obtidas apontam a cobrança de valores entre US\$ 300 e US\$ 600. Não há garantias de que, feito o pagamento, o acesso é restabelecido.

[...]

O Brasil foi um dos países que sentiram os efeitos do ataque. Dentre as empresas locais afetadas estão a sede brasileira da Telefônica/Vivo, em São Paulo, além do Tribunal de Justiça de São Paulo, o Tribunal Regional do Trabalho de São Paulo, o Ministério Público do Estado de São Paulo e o INSS. (GAZETA DO POVO, 2017).

Constata-se que esses trechos ratificam que é a motivação e o propósito que conferem o viés terrorista ao ataque virtual, tendo em vista que a intenção desse ataque global foi causar prejuízo pecuniário por meio da utilização do vírus para sequestrar os computadores e pedir resgate em criptomoedas. Além disso, observa-se que as organizações públicas e privadas do Brasil apresentam sérias falhas de segurança da informação, considerando que tiveram que desligar os computadores ou desconectá-los da rede para impedir o ataque.

Enfim, o terrorismo cibernético apresenta evolução mediante novos ataques ou ameaças de ataques que surgem, frequentemente, contra computadores, sistemas e redes de computadores no ciberespaço, causando prejuízos, por exemplo, econômicos, em que o computador é a principal arma do terrorismo cibernético. Nesse sentido, o ciber terrorismo requer um maior cuidado da gestão de segurança da informação para a continuidade do negócio das empresas, bem como para a manutenção da prestação de serviços pelas instituições públicas. Diante do exposto, trata-se dos resultados e análise de dados deste estudo no próximo capítulo.

4 ANÁLISE DOS DADOS E RESULTADOS

Este capítulo apresenta os resultados e a análise dos dados coletados por meio de formulário, composto por treze questões, que se encontra no apêndice B desta dissertação. Ressalta-se que o referido instrumento de pesquisa foi aplicado a dezesseis participantes voluntários do setor de tecnologia da informação de oito organizações do Estado da Paraíba.

Os participantes são especialistas ou são responsáveis pela segurança da informação de suas respectivas organizações. Tanto os participantes quanto suas instituições de trabalho terão suas identidades preservadas. Dessa maneira, os participantes foram identificados nesta pesquisa mediante a nomenclatura que segue: participante 1 (P1); participante 2 (P2); participante 3 (P3), e assim por diante.

Para atingir os objetivos planejados, a apresentação dos resultados e a análise dos dados ocorrerão através de três etapas subsequentes: delimitação do sistema e do ambiente estudado; identificação e análise das variáveis e dos atores; e a construção dos cenários possíveis.

4.1 DELIMITAÇÃO DO SISTEMA E DO AMBIENTE ESTUDADO

Esta etapa mostra um diagnóstico da situação da segurança da informação nas organizações estudadas, destacando as ameaças à segurança da informação; em especial o ciber terrorismo. Para tanto, foi apreendido a percepção dos participantes da área de tecnologia da informação mediante análise das respostas de dez questões iniciais.

As questões apresentam a proposta de aplicabilidade em organizações públicas ou privadas, em que os participantes poderiam responder com base em seu conhecimento da área ou por meio da sua experiência prática.

Com o intuito de compreender a situação da segurança da informação das organizações pesquisadas, foram feitos três questionamentos aos participantes.

No primeiro questionamento, **“As organizações contemporâneas necessitam de Gestão de Segurança da Informação no ciberespaço?”**, busca-se entender se a GSI é um elemento indispensável para as organizações da atualidade

a partir da percepção de seus colaboradores (servidores, empregados e trabalhadores). Observa-se que 93,75% dos participantes concordam totalmente de que a GSI é fundamental para a gestão das organizações públicas ou privadas. Ou seja, apenas o participante 13 (6,25%) discordou totalmente dessa percepção. Essa porcentagem ratifica a informação como um bem ou um ativo organizacional e a GSI como vital e estratégica para a existência das organizações investigadas.

Na segunda indagação, **“A sua organização está preparada para assegurar os princípios básicos da segurança da informação no atual contexto de avanço tecnológico?”**, procura-se visualizar a situação da segurança da informação das instituições participantes da pesquisa. Verificou-se que 62,5% dos participantes aceitam de forma parcial que suas organizações conseguem garantir a confidencialidade, integridade e disponibilidade da informação. Por outro lado, 37,5% dos participantes discordam parcialmente dessa compreensão. Nesse contexto, verifica-se que as organizações estão preocupadas com a segurança da informação diante da evolução das tecnologias, mas não podem garantir a preservação dos princípios basilares com exatidão e totalidade. Isso se deve a existência de vulnerabilidades ou a sofisticação das formas de ataques virtuais, que impossibilita a detecção e a correção imediata; e/ou por causa de outras motivações não identificadas neste estudo.

Na terceira questão, **“Existe uma política de segurança da informação em sua organização?”**, pretende-se conhecer se as organizações possuem diretrizes, normas e procedimentos voltados para a manutenção da segurança da informação. Constata-se que 50% dos participantes confirmam plenamente a existência de uma política de segurança em suas organizações. Percebe-se também que 31,25% dos participantes concordaram de modo relativo. Além disso, os participantes 1 e 2 (12,5%) discordam totalmente de que há uma política de segurança da informação em sua organização, bem como o participante 13 (6,25%) discordou de maneira parcial. Dessa maneira, entende-se que há uma política de segurança da informação na maioria das organizações, que participaram da pesquisa, ratificando-a como um elemento indispensável para a obtenção dos objetivos organizacionais.

Nessa perspectiva, pode-se assegurar que para uma gestão da segurança da informação, a política é necessária para o alcance de seus objetivos. Contudo, observou-se que não existe uma convicção de que a GSI das organizações pesquisadas é efetiva na proteção dos princípios fundamentais da segurança da

informação.

Em relação às ameaças à segurança da informação, foram utilizadas as questões quatro e cinco a seguir para interpretar a conjuntura das organizações modernas.

Na quarta questão, **“A ausência de uma definição clara acerca das ameaças prejudica a segurança da informação das organizações contemporâneas?”**, obteve-se como resultados: 81,25% dos participantes concordaram de maneira total; o participante 4 (6,25%) não concordou, nem discordou; o participante 7 (6,25%) concordou parcialmente; e o participante 13 (6,25%) discordou totalmente.

Esses resultados ratificam que é necessário delimitar as ameaças para melhor combatê-las, haja vista que a maioria dos participantes aponta que a falta de uma definição óbvia das ameaças é um obstáculo para a criação de mecanismos de proteção da informação nas organizações analisadas.

Na quinta pergunta, **“A maioria dos ataques cibernéticos ocorre pelo fato de existir uma estreita relação entre tecnologias, processos e pessoas?”**, pretende-se compreender se há alguma fragilidade nessa relação, que possibilita a ocorrência de ataques virtuais. Verifica-se que 56,25% dos participantes concordaram parcialmente. Além disso, foram indicadas outras percepções como: 18,75% dos participantes concordaram plenamente; 18,75% discordaram totalmente; e o participante 5 (6,25%) não concordou, nem discordou.

A partir desses resultados, entende-se que os participantes indicam a relação próxima de tecnologias, e também de processos e pessoas como uma vulnerabilidade susceptível de acontecer ataques virtuais. Todavia, essa compreensão é moderada e vaga, ou seja, não apresenta convicção, tendo em vista que a maior parte dos participantes concordaram parcialmente. No contexto organizacional, essa estreita relação deveria garantir a segurança da informação, combatendo as ameaças. Contudo, pode ser a porta de entrada. Provavelmente, isso ocorre pelo fato das pessoas serem consideradas o elo mais frágil dessa relação. (SÊMOLA, 2014).

Na sexta questão, **“Coloque em ordem a ameaça à segurança da informação mais recorrente nas organizações contemporâneas?”**, busca-se identificar e organizar da ameaça mais frequente para a menos frequente, analisando os seguintes grupos de ameaças: naturais; involuntárias; e voluntárias.

Foi atribuído valores de 1 a 3 para ordenar as ameaças através de um critério gradativo. A tabela 1 apresenta os dados e os resultados desse exame.

Tabela 1 – Análise da ordem da ameaça mais comum no contexto organizacional

PARTICIPANTES	AMEAÇAS		
	Naturais	Involuntárias	Voluntárias
P1	2	1	3
P2	2	1	3
P3	3	1	2
P4	2	3	1
P5	2	3	1
P6	3	1	2
P7	3	2	1
P8	3	1	2
P9	3	1	2
P10	3	1	2
P11	3	1	2
P12	3	2	1
P13	3	1	2
P14	2	1	3
P15	3	2	1
P16	3	1	2
	Moda (M _o)= 3	Moda (M _o)= 1	Moda (M _o)= 2

Fonte: Dados da pesquisa (2018).

Os dados da tabela 1 foram analisados de forma estatística por meio da utilização da Moda (M_o) como medida matemática. A Moda consiste no número que mais aparece em um conjunto de dados estatísticos.

Nessa perspectiva, nota-se que cada participante informou a sua ordem de 1 a 3 para os grupos de ameaças, em que os resultados indicam as ameaças involuntárias (inconscientes, causadas pelo desconhecimento) como as mais recorrentes, em seguida, as ameaças voluntárias (propositais, causadas pelo ser humano), e, por fim, as ameaças naturais (decorrentes de fenômenos naturais); tendo em vista que as suas Modas foram, respectivamente, 1 (involuntárias) , 2 (voluntárias) e 3 (naturais).

No que se refere ao fenômeno ciber terrorismo, foram realizados dois questionamentos (questões sétima e oitava) aos participantes para compreender suas opiniões acerca do referido evento.

Na sétima indagação, **“Você conhece organizações contemporâneas que sofreram ataques de natureza ciber terrorista?”**, busca-se conhecer o entendimento dos participantes a partir de eventos ocorridos em organizações modernas. Verifica-se que 75% dos participantes responderam sim, ou seja, sabem

o significado dos ataques ciber terroristas, identificando situações ocorridas no contexto organizacional. Desses participantes, apenas o 7 e o 13 comentaram que os ataques foram em organizações de João Pessoa. Além disso, a questão apresenta outros resultados como: 18,75% dos participantes responderam que não conhecem organizações que sofreram ataques do terrorismo cibernético; e o participante 8 (6,25%) não respondeu a referida questão.

No oitavo questionamento, **“Coloque em ordem a motivação de um ataque de natureza ciber terrorista?”**, pretende-se ratificar as motivações de um ataque ciber terrorista, identificadas no levantamento bibliográfico, mediante a percepção dos participantes, que informaram sua ordem atribuindo valores de 1 a 4. Os dados e os resultados são mostrados na tabela 2.

Tabela 2 – Análise da ordem da motivação de um ataque Ciber terrorista

PARTICIPANTES	MOTIVAÇÃO			
	Política	Social	Ideológica	Financeira
P1	2	4	1	3
P2	3	4	1	2
P3	2	4	3	1
P4	3	2	4	1
P5	3	4	2	1
P6	2	4	3	1
P7	2	4	3	1
P8	3	4	2	1
P9	3	4	1	2
P10	3	4	2	1
P11	3	4	2	1
P12	2	4	1	3
P13	2	3	4	1
P14	2	3	4	1
P15	2	3	4	1
P16	3	4	2	1
	Moda (M _o)= 2 ou 3	Moda (M _o)= 4	Moda (M _o)= 2	Moda (M _o)= 1

Fonte: Dados da pesquisa (2018).

Verifica-se que, na tabela 2, também foi feito um estudo estatístico por meio da Moda. Obteve-se os seguintes resultados: M_o 1 para a motivação financeira; M_o 2 para a ideológica; M_o 2 ou 3 para a política (mesmo valor); e M_o 4 para a social. Percebe-se que a motivação política apresentou dois resultados possíveis, mas se classifica como ordem 3 de motivação, pois a segunda é a ideológica, conforme tabela 2. Assim, de acordo com a percepção da maioria dos participantes, as motivações do ciber terrorismo possuem a seguinte ordem: financeira (1); ideológica

(2); política (3); e social (4).

Em relação às medidas contrárias ao ciber terrorismo, foram utilizadas as questões nove e dez a seguir.

No nono questionamento, “**Coloque em ordem as medidas de segurança contra o ciber terrorismo?**”, pretende-se propor medidas de prevenção e de combate contra os ataques ciber terroristas mediante a percepção dos participantes, que informaram sua ordem atribuindo valores de 1 a 5. Os dados e os resultados são mostrados na tabela 3.

Tabela 3 – Análise da ordem das medidas de proteção e combate aos ataques ciber terroristas

PARTICIPANTES	MEDIDAS DE PROTEÇÃO E COMBATE CONTRA OS ATAQUES CIBER TERRORISTAS				
	Contínuas atualizações de sistema, softwares e aplicativos	Treinamentos de pessoal	Processos organizacionais estabelecidos	Termos de documentação organizacionais que responsabilizem os colaboradores	Legislação
P1	3	1	2	4	5
P2	1	2	3	4	5
P3	3	2	1	4	5
P4	5	2	1	4	3
P5	1	3	2	5	4
P6	1	2	4	5	3
P7	3	2	1	5	4
P8	2	1	3	5	4
P9	1	2	4	5	3
P10	1	2	3	5	4
P11	3	2	1	4	5
P12	2	3	1	4	5
P13	4	5	3	1	2
P14	3	2	1	4	5
P15	-	-	-	-	-
P16	4	5	3	2	1
	Moda (M ₀)= 3	Moda (M ₀)= 2	Moda (M ₀)= 1	Moda (M ₀)= 4	Moda (M ₀)= 5

Fonte: Dados da pesquisa (2018).

Percebe-se que, na tabela 3, foi realizada a análise dos valores citados pelos participantes através da Moda, seguindo o mesmo critério das tabelas anteriores. Ressalta-se que os números citados pelo P15 foram desconsiderados, pois o referido participante repetiu o número para todas as medidas propostas. Nessa perspectiva, os participantes indicam a seguinte sequência para as medidas de proteção e de combate contra o ciber terrorismo:

- 1) **Processos organizacionais estabelecidos;**
- 2) **Treinamentos de pessoal;**
- 3) **Contínuas atualizações de sistema, *softwares* e aplicativos;**

- 4) Termos e documentação organizacionais que responsabilizem os colaboradores;
- 5) Legislação.

Na décima questão, “**Cite outras medidas de prevenção e/ou combate ao ciber terrorismo?**”, buscaram-se outras sugestões dos participantes. Apenas seis participantes responderam esta questão: **P2** sugeriu uma maior divulgação da definição de ciber terrorismo para todos que tem acesso as TICs; **P5** propôs o investimento contínuo em infraestrutura de TI; **P6** recomendou uma aplicação efetiva da política de segurança da informação; **P9** apontou que é necessário uma equipe dedicada em realizar testes de segurança em todas as camadas da infraestrutura de TI; **P12** indicou investimentos em equipamentos e cooperações com fornecedores; **P13** propôs o *checking* dos fatos, segurança da informação por meio de senhas e criptografia, bem como acompanhamento dos dados mediante protocolo de rede.

Após essa descrição e apreciação de dados e resultados referente à situação da segurança da informação, das ameaças e das medidas contra o ciber terrorismo nas organizações pesquisadas, passa-se para a próxima seção, que identifica e analisa as variáveis e os atores deste estudo.

4.2 IDENTIFICAÇÃO E ANÁLISE DAS VARIÁVEIS E DOS ATORES

Seguindo o percurso metodológico, esta segunda etapa do método de Godet descreve e analisa o grau de influência direta de uma variável sobre a outra por meio da análise estrutural, recebendo o auxílio do *software* MICMAC; bem como apresenta e aprecia o grau de influência que um ator exerce sobre o outro e o grau de relevância do objetivo em relação aos atores. Estes são analisados com o *software* MACTOR.

Esta fase, comumente, acontece através de reuniões ou oficinas, buscando o consenso das respostas dos participantes. Todavia, ressalta-se que foi necessário fazer adaptações na coleta e na análise dos valores estatísticos para se adequar a amostra intencional por conveniência e a ferramenta de pesquisa, tendo em vista que a coleta ocorreu em oito lugares distintos.

Dessa maneira, foi realizada uma análise estatística dos dados numéricos

contidos nas matrizes do instrumento da pesquisa, elaboradas de acordo com os *softwares* MICMAC e MACTOR. A medida utilizada também foi a Moda (M_o), mantendo a coerência da proposta do método, que preconiza o consenso dos valores pelo grupo pesquisado.

As variáveis, os atores e os objetivos foram identificados e definidos com base no levantamento bibliográfico e no contexto organizacional.

Para o alcance dos objetivos planejados para esta etapa, foi empregado o formulário na coleta dos dados, questões: décima primeira; décima segunda; e décima terceira.

Diante do exposto, os dados foram examinados nos seguintes passos: análise estrutural das variáveis e análise da relação de atores.

4.2.1 Análise estrutural das variáveis

Inicialmente, ocorreu a determinação das variáveis de acordo com a revisão da literatura e do contexto organizacional abordado. As variáveis foram inseridas em uma matriz de análise estrutural, que foi a décima primeira questão do instrumento de coleta de dados (formulário). A matriz de análise estrutural deste estudo, que é constituída por cinco variáveis, foi preenchida pelos participantes da pesquisa de forma qualitativa, seguindo o que propõe o método de Godet.

Nessa perspectiva, os participantes preencheram a referida matriz para verificar o grau de influência direta de uma variável sobre a outra, atribuindo os seguintes valores: **(0) sem influência direta; (1) fraca; (2) média; (3) forte; e (P) potenciais**, que podem acontecer em algum momento futuro.

Os dados obtidos foram analisados de forma estatística através da Moda. Para tanto, substituiu-se o P de potenciais por 4 para calcular o valor da M_o . Em seguida, os dados foram transcritos para o *software* MICMAC, possibilitando identificar a influência e a dependência das variáveis na forma de gráficos e mapas, que podem mostrar relações diretas, indiretas e potenciais das variáveis. Neste estudo, apresentam-se adiante as relações diretas das variáveis. O quadro 6 apresenta como a variável está inserida no MICMAC.

Quadro 6 – Número, variável, abreviatura e descrição no MICMAC

Nº	Variável	Abreviatura	Descrição da variável
1	Políticas Públicas	Pol. Pub.	Ações ou programas elaborados pelo Estado por meio de seus representantes.
2	Ideologias	Ideol.	Ideias ou pensamentos (políticos, sociais, religiosos, etc.) individuais ou coletivos.
3	Mercado	Merc.	Espaço virtual e social de negociações de vendedores e compradores.
4	Tecnologias	Tec.	Técnicas, ferramentas, processos, entre outros.
5	Vantagem Indevida	Vant. Ind.	Recebimento de benefícios através de procedimentos ilegais, como a corrupção.

Fonte: Elaborado pelo autor (2018).

Nessa perspectiva, a matriz foi preenchida com os valores predominantes nas respostas dos dezesseis participantes. A figura 4 mostra como os valores ficaram na matriz do aplicativo MICMAC.

Figura 4 – Matriz de influências diretas das variáveis no aplicativo MICMAC

	1 : Pol. Pub.	2 : Ideol.	3 : Merc.	4 : Tec.	5 : Vant. Ind.
1 : Pol. Pub.	0	3	3	1	2
2 : Ideol.	3	0	1	2	1
3 : Merc.	3	2	0	3	2
4 : Tec.	1	2	3	0	2
5 : Vant. Ind.	3	2	2	3	0

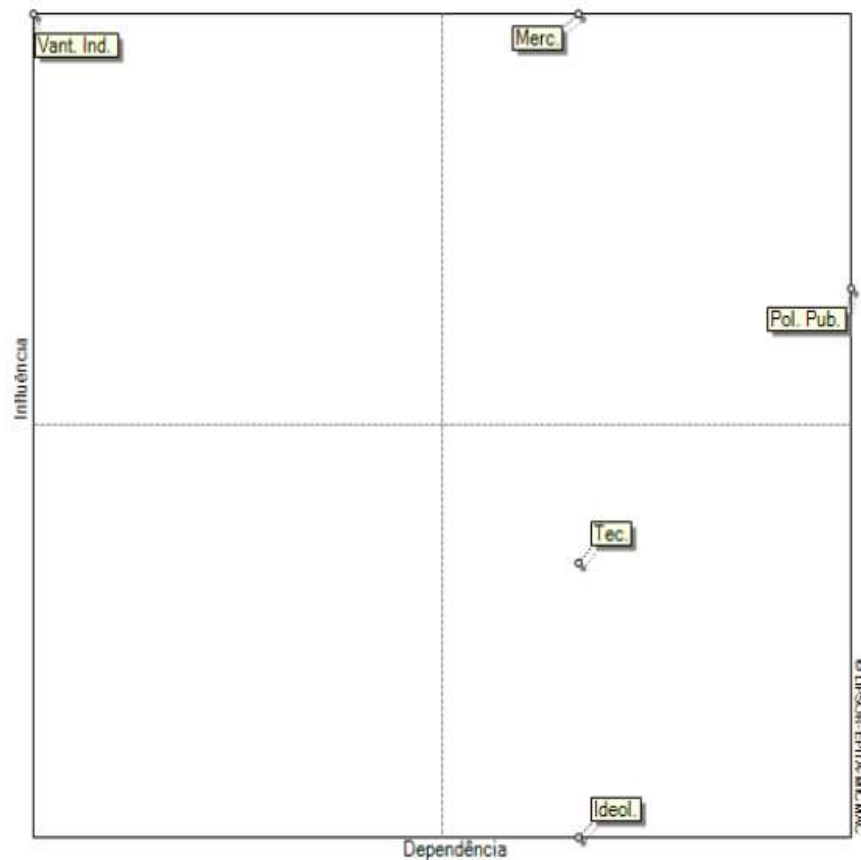
© LIPSOR-EPTA-MICMAC

Fonte: Dados da pesquisa gerados pelo *software* MICMAC (2018).

Nota-se que os valores constantes na matriz são as Modas dos conjuntos de valores citados pelos participantes para a relação de cada variável da referida matriz, que possibilita ao MICMAC compreender o grau de influência e dependência dessas variáveis, corroborando para a construção dos prováveis cenários deste estudo.

Nesse contexto, a partir da utilização do aplicativo MICMAC, tem-se o mapa de influências/dependências diretas das variáveis como produto. A figura 5 mostra o referido mapa.

Figura 5 – Mapa de influências/dependências diretas das variáveis

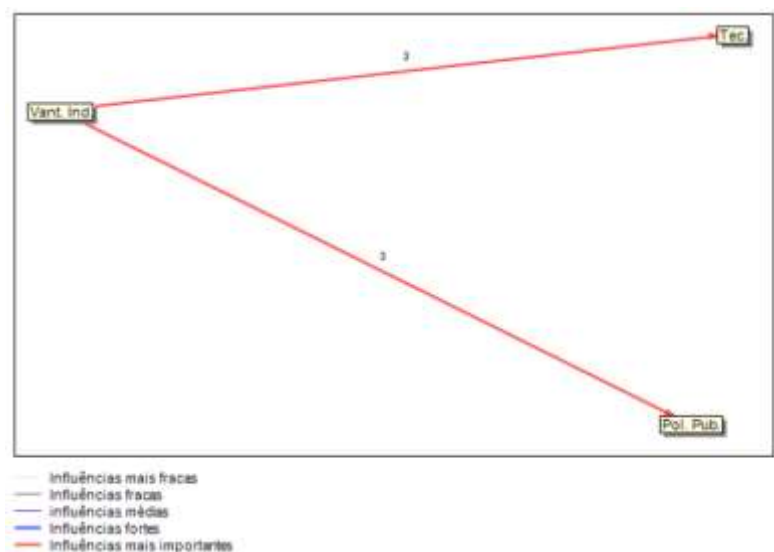


Fonte: Dados da pesquisa gerados pelo software MICMAC (2018).

Na figura 5, percebe-se que **Vantagem Indevida** é a variável de maior influência e pouca dependência, estando localizada no quadro de cima do lado esquerdo. As variáveis **Mercado e Políticas Públicas**, que estão no quadro de cima do lado direito, são as de maior influência e maior dependência. As variáveis **Tecnologias e Ideologias**, por sua vez, que estão no quadro de baixo do lado direito, são pouco influentes e muito dependentes. Nota-se também que não há variáveis poucos influentes e poucos dependentes, ou seja, localizadas no quadro de baixo do lado esquerdo.

Além disso, tem-se as influências de variáveis mais importantes como resultado da análise através do aplicativo MICMAC, de acordo com o gráfico 4 que segue:

Gráfico 4 – Influências diretas das variáveis



Fonte: Dados da pesquisa gerados pelo *software* MICMAC (2018).

Constata-se que as influências mais importantes ocorrem através da relação entre as seguintes variáveis: **Vantagem Indevida e Tecnologias; e Vantagem Indevida e Políticas Públicas**. Essas relações foram indicadas pelos participantes como as com grau de influência mais forte, tendo em vista que receberam o valor 3.

A partir desses resultados, comprova-se que a **Vantagem Indevida** é a variável mais influente e a mais importante para o desenvolvimento do ciberterrorismo, ratificando as motivações políticas, sociais e financeiras como as principais causas dos ataques ciberterroristas.

Esses resultados corroboram o que foi citado por Ahmad *et al.* (2012), que indicam as possíveis motivações para ataques deste tipo.

Na sequência, passa-se a tratar da análise dos atores, que também são necessários para a construção dos cenários deste estudo.

4.2.2 Análise da relação de atores

De acordo com a proposta do percurso metodológico, a análise de atores é a segunda técnica do método prospectivo de Godet, que recebe auxílio do *software* MACTOR para a apreciação dos dados. Esse software utiliza duas matrizes para a análise. A primeira examina o grau de influência que um ator exerce sobre o outro. A segunda analisa as consequências dos objetivos em relação aos atores.

Os atores e os objetivos deste estudo também foram determinados, segundo

a revisão da literatura e do contexto organizacional abordado. Os atores, que são cinco, foram inseridos em uma matriz de análise da relação de atores, que foi a décima segunda questão do formulário de coleta de dados. A outra matriz, inserida na décima terceira questão, foi constituída pelos atores e pelos objetivos, que também foram cinco.

Essas matrizes foram preenchidas pelos participantes da pesquisa conforme suas percepções, cumprindo o que preceitua o método de cenários prospectivos de Godet.

Na matriz de análise do grau de influência de um ator sobre o outro, os participantes fizeram o preenchimento, atribuindo os seguintes valores: **(0) sem influência direta; (1) processos; (2) projetos; (3) missão; e (4) existência.**

Na matriz que verifica se o objetivo tem consequência sobre o ator, os participantes fizeram o preenchimento, atribuindo os seguintes valores: **(0) o objetivo é pouco consequente; (1) o objetivo tem consequências sobre os processos do ator; (2) o objetivo tem consequências sobre os projetos do ator; (3) o objetivo tem consequências sobre a missão do ator; e (4) o objetivo tem consequências sobre a existência do ator.** Ressalta-se que nessa matriz é necessário indicar se o ator é favorável ou desfavorável ao objetivo. Isso foi realizado por meio da inserção do **sinal (+/-) aos números.**

Os dados alcançados também necessitaram de uma análise estatística por meio da Mo. Em seguida, os valores da Moda, isto é, os mais predominantes, foram transferidos para o *software* MACTOR, propiciando uma análise das relações: atores x atores; objetivos x atores. Nesse sentido, o MACTOR apresenta as relações diretas, indiretas, e as posições valoradas dos atores sobre os objetivos na forma de mapas e gráficos. Neste estudo, mostra-se as influências e as dependências entre atores a partir da análise de suas relações diretas e indiretas, bem como demonstra-se as consequências dos objetivos acerca dos atores e as posições valoradas dos atores em relação aos objetivos. O quadro 7 mostra como o ator está inserido no MACTOR.

Quadro 7 – Número, ator, abreviatura e descrição no MACTOR

Nº	Ator	Abreviatura	Descrição do ator
1	Governo	Gov.	Responsável pela administração de um Estado (Federal, Estadual e Municipal).
2	Empresas	Emp.	É constituída por pessoas e materiais, participa no mercado de bens ou serviços,

			objetivando o lucro monetário.
3	Colaboradores	Colab.	Funcionário, empregado, servidor, entre outros.
4	Clientes/Usuários	Client./Us.	Adquire bens ou serviços.
5	Pessoas Externas	Pess. Ext.	Não faz parte de uma organização pública ou privada.

Fonte: Elaborado pelo autor (2018).

O quadro 8, por sua vez, demonstra como os objetivos foram adicionados ao *software* MACTOR, destacando, principalmente, a sua forma abreviada, que consta nos gráficos.

Quadro 8 – Número, objetivo, abreviatura e descrição no MACTOR

Nº	Objetivo	Abreviatura	Descrição do objetivo
1	Elaborar Políticas Públicas	Elab. Pol.	Elaborar políticas públicas sociais, econômicas, etc.
2	Divulgar Ideologias	Div. Ideol.	Divulgar ideologias sociais, políticas, religiosas.
3	Novas Ideias	Nov. Id.	Executar novas ideias de mercado.
4	Uso das Tecnologias	Uso Tec.	Utilizar técnicas, ferramentas, processos, instrumentos.
5	Benefícios Ilícitos	Benef. Il.	Receber benefícios ilegais.

Fonte: Elaborado pelo autor (2018).

No que se refere ao grau de influência direta que um ator exerce sobre o outro, nota-se que os valores inseridos no aplicativo MACTOR representam a Moda do conjunto de valores citados pelos dezesseis participantes. A figura 6 apresenta a matriz criada no MACTOR a partir dos valores predominantes.

Figura 6 – Matriz de influências diretas dos atores no aplicativo MACTOR

MID	Gov.	Emp.	Colab.	Client/Us.	Pess. Ext.
Gov.	0	4	2	1	1
Emp.	2	0	2	4	0
Colab.	2	3	0	1	1
Client/Us.	2	4	2	0	0
Pess. Ext.	2	1	1	0	0

© LIPSOR-EPTA-MACTOR

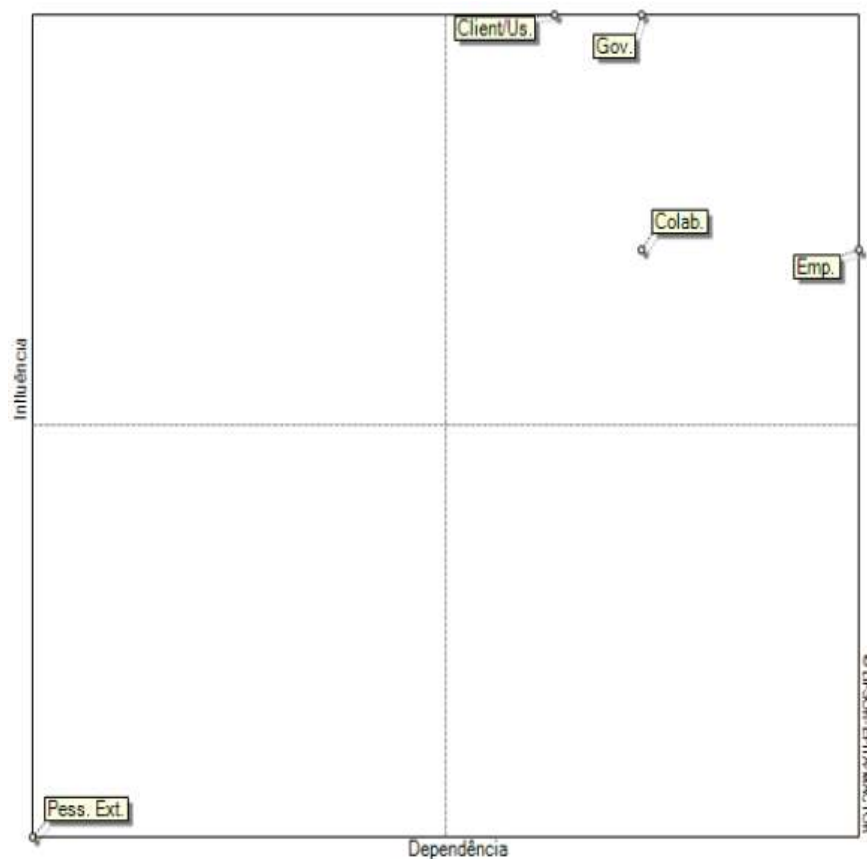
Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

A partir dos dados dessa matriz, o *software* MACTOR calcula de forma automática as influências e as dependências diretas e indiretas entre atores,

possibilitando identificar os atores mais influentes e poucos dependentes, os atores tão influentes quanto dependentes, os mais dependentes com pouca influência, e os que não são dependentes nem influentes. Isso é representado na forma de gráficos e de mapas.

Nesse sentido, a figura 7 mostra o mapa do posicionamento dos atores em relação a suas influências e dependências.

Figura 7 – Mapa de influências e dependências entre atores



Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

Na figura 7, percebe-se que os atores **Clientes/Usuários, Governo, Colaboradores e Empresas** estão posicionados no quadrante direito e acima, sendo classificados como atores de ligação, tendo em vista que são tão influentes quanto dependentes, ou seja, exercem influência e dependem dos demais atores no contexto estudado. O ator **Pessoas Externas** está localizado no quadrante esquerdo e abaixo, sendo categorizados como atores autônomos, ou melhor, não são influentes nem dependentes. Verifica-se também que não há atores dominantes (muito influentes e pouco dependentes), situados no quadrante esquerdo e acima; bem como não existem atores dominados (poucos influentes e muito dependentes), situados no quadrante direito e abaixo.

No que diz respeito à relação entre atores e objetivos, o MACTOR também determina a posição do ator em relação aos objetivos. Isso foi possível por meio da inserção dos valores predominante citados pelos 16 participantes no aplicativo MACTOR. A figura 8 representa a matriz de posições valoradas entre atores e objetivos.

Figura 8 – Matriz de posições valoradas entre atores e objetivos

2MAO	© LIPSOR-EPTA-MACTOR				
	Elab. Pol.	Div. Ideol	Nov. Id.	Uso Tec.	Benef. Il.
Gov.	4	0	3	2	-3
Emp.	2	2	3	4	-4
Colab.	3	1	2	2	-4
Client/Us.	1	0	1	1	-4
Pess. Ext.	0	0	1	1	-4

Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

Nota-se que essa matriz da figura 8 possui os números, que caracterizam a Moda do conjunto de valores citados pelos participantes na questão 13 do formulário. A partir dessa matriz, o aplicativo MACTOR gerou outra matriz mostrando o posicionamento favorável do ator acerca do cumprimento do objetivo através do mais 1, o posicionamento desfavorável por meio do menos 1, e a posição neutra mediante o zero. A figura 9 trata da referida matriz.

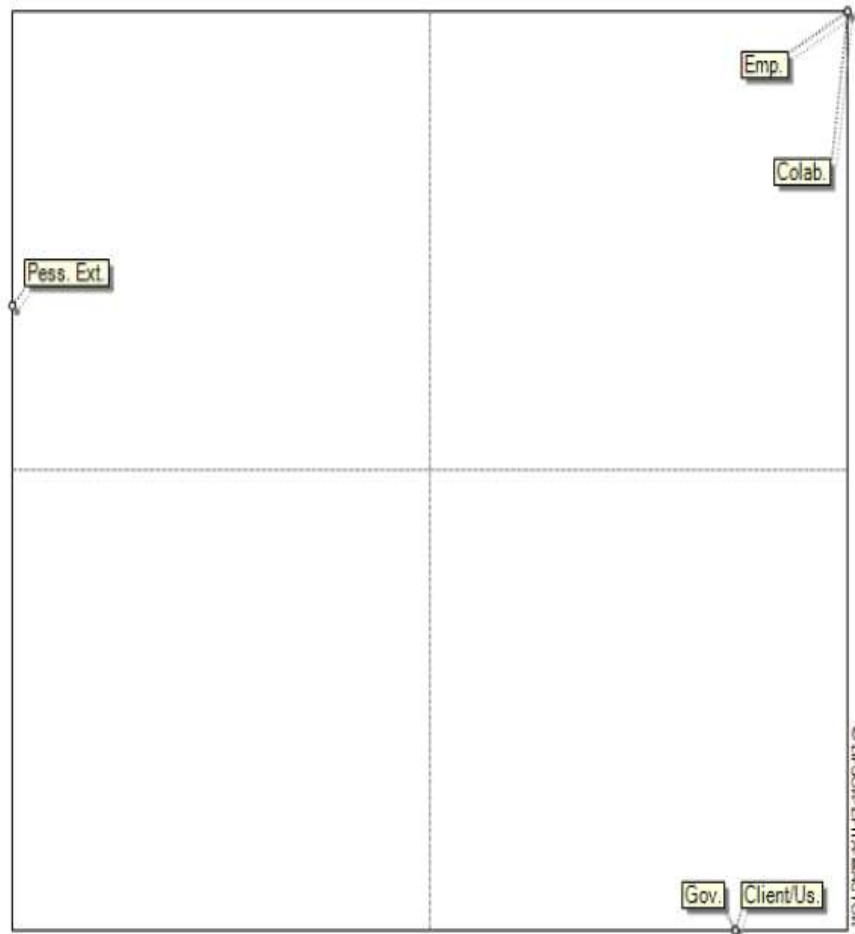
Figura 9 – Matriz de posições simples entre atores e objetivos

1MAO	© LIPSOR-EPTA-MACTOR					
	Elab. Pol.	Div. Ideol	Nov. Id.	Uso Tec.	Benef. Il.	Soma absoluta
Gov.	1	0	1	1	-1	4
Emp.	1	1	1	1	-1	5
Colab.	1	1	1	1	-1	5
Client/Us.	1	0	1	1	-1	4
Pess. Ext.	0	0	1	1	-1	3
Quantidade de acordos	4	2	5	5	0	
Número de discordâncias	0	0	0	0	-5	
Número de posições	4	2	5	5	5	

Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

A partir dessas matrizes, o *software* MACTOR mostra o grau de convergências entre os atores deste estudo, considerando os objetivos indicados. Na figura 10, tem-se o mapa de convergências.

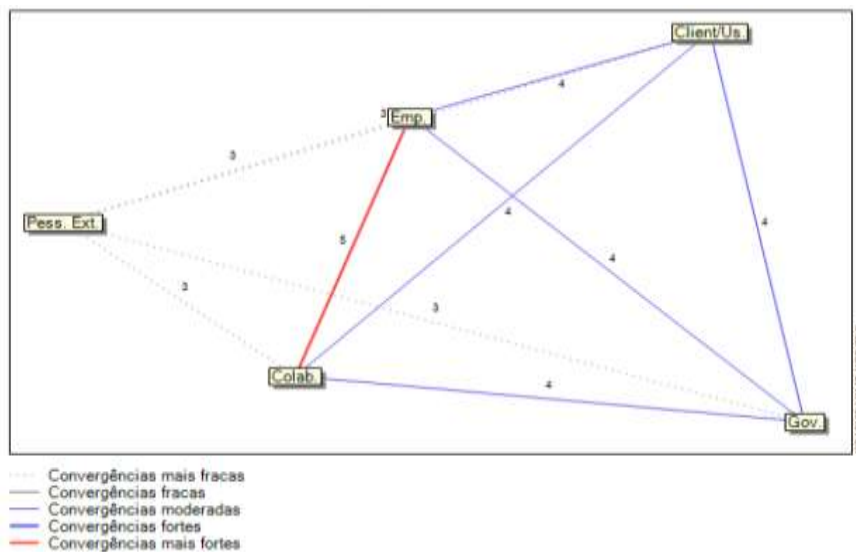
Figura 10 – Mapa de convergências entre atores



Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

Na figura 10, percebe-se que os atores **Empresas e Colaboradores** possuem convergência entre si. Além desses, os atores **Governo e Clientes/Usuários** também apresentam convergência entre si. O ator **Pessoas Externas** encontra-se isolado no mapa. Essas convergências são visualizadas em formato de grafos no gráfico 5.

Gráfico 5 – Convergências entre atores

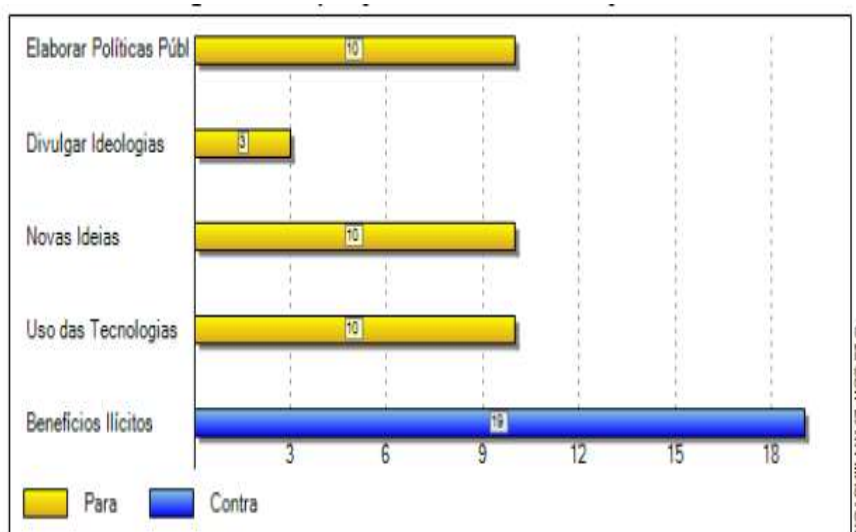


Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

O gráfico 5 apresenta as possibilidades de convergências: mais fortes; fortes; moderadas; fracas; e mais fracas. Nessa perspectiva, verifica-se que os atores **Empresas e Colaboradores** estão destacados no gráfico como mais fortes em relação à convergência, pois têm o maior nível de intensidade. Os atores **Governo e Clientes/Usuários** dispõem de uma convergência moderada entre si e entre os atores **Colaboradores e Empresas**. O ator **Pessoas Externas**, por sua vez, apresenta uma convergência mais fraca em relação a todos os atores deste estudo.

O *software* MACTOR também possibilita visualizar a implicação dos atores em relação aos objetivos, conforme figura 11, apresentada na sequência.

Figura 11 – Histograma da implicação dos atores sobre os objetivos



Fonte: Dados da pesquisa gerados pelo *software* MACTOR (2018).

O histograma da figura 11 demonstra que os objetivos **(Elaborar Políticas Públicas, Novas Ideias e Uso das Tecnologias)** são mais relevantes e expressivos para os atores, implicando de forma positiva e favorável no contexto organizacional em análise. Em seguida, o objetivo **(Divulgar Ideologias)** também possui uma implicação positiva para os atores. Por outro lado, o objetivo **(Benefícios Ilícitos)** apresenta uma implicação negativa e desfavorável para os atores e para o contexto organizacional.

Esses foram os principais resultados indicados pelo *software* MACTOR, que são fundamentais para o desenvolvimento dos prováveis cenários prospectivos para o ciber terrorismo na Paraíba, descritos a seguir.

4.3 CONSTRUÇÃO DOS CENÁRIOS POSSÍVEIS APLICADOS AO CIBER TERRORISMO NA PARAÍBA

A construção de cenários consiste na terceira etapa do método de Godet. Neste estudo, desenvolveram-se três cenários para o ciber terrorismo no contexto organizacional estudado, respaldando-se no levantamento bibliográfico, nos dados e resultados coletados através das respostas dos participantes especialistas do setor de tecnologia da informação das organizações que se disponibilizaram a participar da pesquisa. Além disso, os resultados da análise estrutural das variáveis e da análise da relação dos atores são referências principais para a produção dos cenários deste estudo.

Nessa perspectiva, criaram-se os seguintes cenários: cenário propício ao ciber terrorismo; cenário adverso ao ciber terrorismo; e cenário provável para o ciber terrorismo.

1. **Cenário propício ao ciber terrorismo:** favorável para a realização de ataques de natureza ciber terrorista no âmbito das organizações estudadas. A partir da relação de convergência mais forte entre os atores **empresas** e **colaboradores**, nota-se a possibilidade de um cenário bom para os ataques ciber terroristas no momento em que as **empresas** não fazem investimento em treinamentos e não oferecem uma infraestrutura de tecnologia da informação adequada para seus **colaboradores**, que podem não seguir as políticas de segurança da informação da empresa, tendo em vista sua falta de

conhecimento ou ausência de tecnologias apropriadas, tornando um ambiente vulnerável e conveniente para a atuação do terrorismo cibernético. Verifica-se também a probabilidade deste cenário por meio da relação moderada entre os atores **governo e colaboradores**, quando o **governo** não cria as legislações, as normas e os mecanismos de proteção para o desenvolvimento das atividades de seus **colaboradores**, bem como não os treinam, sequer disponibiliza o uso de tecnologias pertinentes. Isso produz fragilidades na segurança da informação, refletindo nas ações das organizações, tanto públicas quanto privadas, facilitando os ataques ciber terroristas.

2. **Cenário adverso ao ciber terrorismo:** desfavorável para a atuação do ciber terrorismo no contexto estudado. Este cenário é possível, quando as **empresas** realizam investimentos em treinamentos de seus **colaboradores**, disponibilizam uma infraestrutura de tecnologia da informação adequadas para o desenvolvimento das atividades de segurança da informação, determinam os processos organizacionais e produzem termos e documentação organizacionais que responsabilizem os seus **colaboradores**. Estes atores terão ferramentas para cumprir com as políticas de segurança da informação das **empresas**, realizando as constantes atualizações de *softwares* e aplicativos. Nesse sentido, o cenário torna-se seguro e estável, dificultando a atuação do terrorismo cibernético. Da mesma forma, se o **governo** criar as legislações, as normas e os mecanismos de proteção, fomentando a segurança da informação, para a realização das atividades de seus **colaboradores**, oportunizando os meios necessários e adequados. Isso se reflete, positivamente, nas ações das organizações públicas e privadas, na proporção em que apresenta um cenário seguro e consistente, tornando-se impróprio para a prática ciber terrorista.
3. **Cenário provável para o ciber terrorismo:** crescimento gradativo dos ataques de cunho ciber terrorista no âmbito das organizações estudadas. Neste cenário, as **empresas** passam a não ter mais interesse em elaborar legislação, normas e diretrizes acerca da segurança da informação, bem como não oferecem mais os recursos de tecnologia da informação necessários para seus **colaboradores** assegurarem os princípios básicos da segurança da informação. Do mesmo modo, o **governo** passa a não produzir legislação ou atualizar suas legislações, não cria as normas e os mecanismos

de proteção, bem como não determina os seus processos organizacionais, referentes à segurança da informação. Enfim, o **governo** não fomenta a segurança da informação, repercutindo, negativamente, nas ações das organizações, tanto públicas quanto privadas, e de seus **colaboradores**. Além disso, tanto as empresas quanto o governo não asseguram um produto ou um serviço satisfatório para seus **clientes ou usuários**. Nessa perspectiva, verifica-se que a variável **vantagem indevida**, na forma de corrupção ou com outra finalidade ilícita, pode ser inserida neste cenário, pois está influenciando diretamente as **tecnologias** e as **políticas públicas** no sentido de não utilização ou elaboração pelas **empresas** e pelo **governo**. Nota-se que há uma tendência de um aumento expressivo de ataques ciber terroristas, sendo praticados inclusive por atores como: **empresas; governo; colaboradores; clientes/usuários; e pessoas externas**. Estes atores buscam em comum benefícios ilícitos neste cenário provável.

Esses foram os prováveis cenários para o ciber terrorismo nas organizações estudadas na Paraíba, construídos com base na revisão da literatura e a partir dos dados coletados por meio de formulário, bem como através das análises dos *softwares* MICMAC e MACTOR. Passa-se a tecer as considerações finais a seguir.

5 CONSIDERAÇÕES FINAIS

A informação adquiriu valor patrimonial para as instituições públicas e privadas, devido à utilização de tecnologias digitais, como o computador e a internet, que propiciam celeridade no processamento e na tramitação da informação no ciberespaço. As tecnologias digitais não são neutras ou imparciais, tendo em vista que modificam a realidade das organizações na medida em que são empregadas como suporte fundamental para as diversas atividades desenvolvidas no contexto organizacional.

A maioria das organizações apresentam vulnerabilidades em seus sistemas de informação. Tais fragilidades podem ser de ordem física, natural, *hardware*, *software*, mídias, comunicação e humanas. Ou seja, há diversas formas de acesso para a exploração das ameaças.

No ciberespaço, há também as ameaças à segurança da informação como o ciber terrorismo, que utiliza as tecnologias digitais para realizar seus ataques. O terrorismo cibernético segue o avanço tecnológico, apresentando evolução mediante novos ataques ou ameaças de ataques que surgem frequentemente, bem como aumentou significativamente nos últimos anos. Esse fenômeno torna-se complexo e de difícil compreensão no contexto organizacional, dificultando a criação de mecanismos adequados de proteção e defesa pelo setor de segurança da informação dos órgãos.

Nessa perspectiva, a pesquisa pretendeu responder à questão que segue:

Como estão os cenários sobre o ciber terrorismo na Paraíba?

Para isso, projetou-se como objetivo geral estudar cenários prospectivos sobre o ciber terrorismo neste Estado. De maneira específica, pretendeu-se: identificar as variáveis e os atores do ciber terrorismo no contexto organizacional; examinar a interação das variáveis e dos atores; construir os prováveis cenários; e propor ações de proteção e combate contra o terrorismo cibernético.

A revisão da literatura foi essencial, pois possibilitou o conhecimento de conceitos e características relacionados à Gestão da Segurança da Informação e ao ciber terrorismo, mostrando as principais formas de ataques virtuais que ocorrem no Brasil.

Nesse sentido, verificou-se que as organizações incorporaram a segurança da informação em suas gestões, como uma forma necessária para a proteção de

seus negócios e seus objetivos organizacionais. Outrossim, a maioria das organizações públicas ou privadas possuem um setor, que gerencia a segurança da informação do contexto organizacional, definindo políticas de segurança, ou seja, normas, diretrizes, princípios, procedimentos e sanções.

Notou-se também que há uma gestão da segurança da informação nas instituições, que é tratada como estratégica para assegurar os princípios fundamentais da segurança da informação: confidencialidade; integridade e disponibilidade.

Para alcançar o propósito principal deste estudo, fundamentou-se em uma metodologia de cenários prospectivos, que foi a do Michel Godet. Nesse sentido, utilizou-se as três etapas da metodologia: delimitação do sistema e do ambiente estudado; identificação e análise das variáveis e dos atores; e a construção dos eventuais cenários.

Empregou-se o formulário como instrumento de coleta de dados, elaborando indagações sobre segurança da informação, acerca das ameaças e a respeito do ciber terrorismo. Além disso, utilizou-se algumas matrizes específicas do método de Godet no formulário. A coleta ocorreu na forma presencial, em que o formulário foi aplicado a uma **amostra intencional por conveniência** composta por **dezesseis participantes** (servidores ou empregados do setor de TI), sendo **2 (dois)** de cada setor que autorizou a coleta dos dados.

Além disso, foram utilizados os *softwares* MICMAC e MACTOR, que são específicos do método de Godet, para a análise das variáveis e dos atores. Os dados que foram inseridos aos respectivos aplicativos passaram por um tratamento estatístico através da medida estatística Moda.

Em relação aos principais resultados da pesquisa, constatou-se que a maioria dos participantes indicam que a GSI é essencial para as organizações contemporâneas. Contudo, os participantes demonstram que suas organizações não estão, plenamente, preparadas para assegurar os princípios básicos da segurança da informação. Da mesma forma, apenas 50% dos participantes responderam que existe uma política de segurança da informação em suas instituições.

Os resultados também possibilitam ratificar que a falta de uma definição e a ausência de características das ameaças dificultam a criação de providências de combate pela Gestão da Segurança da Informação das organizações. Os participantes apontam que as ameaças involuntárias são as mais comuns, seguidas

das voluntárias, e, por fim, as ameaças naturais.

Verificou-se que existe um crescimento expressivo do ciber terrorismo na Paraíba. Isso foi confirmado pela maioria dos participantes, que conhecem organizações que sofreram ataques dessa natureza, inclusive, o P7 e o P13 informaram que os ataques ocorreram em João Pessoa. Além disso, os participantes indicam que a principal motivação para os ataques ciber terroristas é a financeira, seguida pela ideológica, pela política e pela social.

Em relação às variáveis do ciber terrorismo, Políticas Públicas, Ideologias, Mercado, Tecnologias e Vantagem Indevida foram definidas como variáveis do contexto organizacional. Essas variáveis foram analisadas pelo *software* MICMAC, que destacou Vantagem Indevida como a variável mais influente. Do mesmo modo, a influência mais importante ocorreu através das variáveis Vantagem Indevida e Tecnologias, e Vantagem Indevida e Políticas Públicas. Essa ênfase na variável Vantagem Indevida confirma que a principal motivação dos ataques ciber terroristas é a financeira.

No que diz respeito aos prováveis atores e objetivos do ciber terrorismo nas organizações, Governo, Empresas, Colaboradores, Clientes/Usuários e Pessoas Externas podem ser definidos como atores. Os objetivos, por sua vez, foram Elaborar Políticas Públicas, Divulgar Ideologias, Novas Ideias, Uso das Tecnologias e Benefícios Ilícitos. Os atores e os objetivos foram apreciados pelo *software* MACTOR.

O *software* MACTOR mostrou que os atores Governo, Empresas, Colaboradores e Clientes/Usuários são tão influentes quanto dependentes. O aplicativo indicou também que a convergência mais forte acontece entre Colaboradores e Empresas, sendo mais provável um ataque ciber terrorista através dessa relação. O ator Pessoas Externas, por sua vez, apresenta autonomia para realizar os ataques de natureza ciber terrorista, haja vista que não possui influência nem dependência e sua convergência é mais fraca com os demais atores. Outrossim, o *software* MACTOR apontou que o Benefício Ilícito é o objetivo que tem uma implicação negativa para os atores. Ou seja, é o que pode facilitar a um ataque ciber terrorista ou de outra natureza.

Nessa perspectiva, a partir da relação de convergência mais forte e moderada entre os atores e através da influência mais forte entre as variáveis, este estudo construiu os seguintes cenários para o ciber terrorismo nas organizações estudadas

na Paraíba: cenário propício; cenário adverso; e cenário provável.

Para alcançar o propósito do quarto objetivo, sugerem-se as medidas de combate ou proteção contra o ciber terrorismo, confirmadas e ordenadas pelos participantes durante a coleta dos dados, como ações necessárias para a gestão da segurança da informação. Dessa maneira, alguns riscos de segurança da informação foram identificados a partir das respostas dos participantes e da análise das variáveis e dos atores nos aplicativos MICMAC e MACTOR. A correlação entre riscos e ações são mostradas no quadro 9.

Quadro 9 – Ações para a gestão da segurança da informação das organizações.

Nº	Riscos	Ações necessárias
1	Inexistência de um processo organizacional.	Processos organizacionais estabelecidos.
2	Colaboradores que desconhecem a política de segurança de sua organização.	Treinamentos de pessoal.
3	Sistemas, aplicativos e <i>softwares</i> desatualizados.	Contínuas atualizações de sistema, <i>softwares</i> e aplicativos.
4	Inexistência de regras que responsabilizem os colaboradores.	Termos e documentação organizacionais que responsabilizem os colaboradores.
5	Inexistência de legislação de segurança da informação.	Legislação.
6	Falta investimento em infraestrutura de tecnologia da informação.	Investimento contínuo em infraestrutura de tecnologia da informação.
7	Inexecução da política de segurança da informação.	Aplicação efetiva da política de segurança da informação.
8	Colaboradores trabalham isoladamente.	Equipe para realizar teste de segurança em todas as camadas da infraestrutura de tecnologia da informação.

Fonte: Elaborado pelo autor (2018).

Enfim, este estudo desenvolveu eventuais cenários sobre o ciber terrorismo, que podem permanecer em uma situação futura na Paraíba, para auxiliar as organizações no combate de tal fenômeno. Dessa maneira, a pesquisa tem o propósito de contribuir com a Gestão da Segurança da Informação e setores relacionados no contexto organizacional.

Apesar do estudo focar em oito organizações da Paraíba, a amostra é representativa e a construção dos cenários prospectivos sobre o ciber terrorismo mostrou-se complexa e ampla, podendo serem aplicados em qualquer organização nacional ou mundial. Além do mais, os cenários demonstraram-se ser um

instrumento de utilidade na compreensão do ciber terrorismo no contexto organizacional.

No geral, os resultados indicam que as organizações estudadas têm consciência da relevância da segurança da informação para garantir a manutenção de seus processos, seus projetos, sua missão e sua existência. Todavia, as respostas dos participantes também indicam que há falhas ou vulnerabilidades que podem ser exploradas por ameaças como o ciber terrorismo. Outro ponto identificado foi que as organizações não têm mecanismos para tratar as vulnerabilidades, mesmo tendo consciência do problema, não foi constatado ações que possam tratar tal situação. O que sugere que tais organizações continuarão vulneráveis a estes tipos de ataques.

Assim, este estudo pode ser fonte de inspiração para futuras pesquisas do Programa de Pós-Graduação em Organizações Aprendentes e para estudos de outros programas.

REFERÊNCIAS

AGUIAR, Poliana Policarpo de Magalhães; BRENNAND, Edna Gusmão de Góes. **Cibercrimes na E-democracia**. Belo Horizonte: D'Plácido, 2016.

AHMAD, Rabiah; YUNOS, Zahri. The Application of Mixed Method in Developing a Cyber Terrorism Framework. **Journal of Information Security**, 3, p. 209-214, 2012.

AHMAD, Rabiah *et al.* Perception on Cyber Terrorism: A Focus Group Discussion Approach. **Journal of Information Security**, 3, p. 231-237, 2012.

ALAIMO, Michael; TONG, Yonghong. A Comparison Study of International Terrorism Using Geographic Information Systems. **International Journal of Peace Studies**, Volume 22, Number 1, p. 21-37, 2017.

ALBAHAR, Marwan. Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. **Sci Eng Ethics**, 2017.

ALCÂNTARA, Livia Moreira de. Ciberativismo e a Dimensão Comunicativa dos Movimentos Sociais: repertórios, organização e difusão. **Política & Sociedade** - Florianópolis - Vol. 15 - Nº 34 – p. 315-338, Set./Dez. 2016.

ANG, Peng Hwa; PANG, Natalie. Globalização da Internet, Soberania ou Democracia: o Trilema do Fórum de Governança da Internet. **Revista de Direito, Estado e Telecomunicações**, v. 6, n. 1, p. 45-62, 2014.

ANGELONI, Maria Terezinha. **Organizações do Conhecimento**: infra-estrutura, pessoas e tecnologia. 2 ed. São Paulo: Saraiva, 2008.

ARAÚJO, Carlos Alberto Ávila. Fundamentos da ciência da informação: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 1, p. 57-79, jan./jun. 2014.

ASONGU, Simplicie A.; NWACHUKWU, Jacinta C. The Impact of Terrorism on Governance in African Countries. **World Development**, p. 1-18, 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB ISO/IEC 27002**: Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

AVEN, Terje; GUIKEMA, Seth. On the Concept and Definition of Terrorism Risk. **Risk Analysis**, Vol. 35, No. 12, p. 2162-2171, 2015.

AYRES, Nicholas; MAGLARAS, Leandros A. Cyberterrorism targeting the general public through social media. **Security and Communication Networks**, 9, p. 2864–2875, 2016.

AZEVEDO, Ana. **Marco civil da internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

BARRETO JUNIOR, Irineu Francisco; AULER, Henrique; BARBOSA, Marco Antonio. Hacktivismo e ativismo digital na sociedade da informação. **Redes – Revista Eletrônica Direito e Sociedade**, Canoas, v. 4, n. 2, p. 129-146, nov. 2016.

BELARMINO, Valdete Fernandes; ARAÚJO, Wagner Junqueira de. Análise de vulnerabilidades computacionais em repositórios digitais. **Biblios**, n. 56, p. 1-18, 2014.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência**, Florianópolis, n. 68, p. 109-127, jun. 2014.

BRASIL. **Decreto nº 3.505, de 13 de junho de 2000**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 11 fev. 2017.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 08 fev. 2017.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC. Rede Nacional de Ensino e Pesquisa - RNP. **Cais em Resumo**: alertas, vulnerabilidades e incidentes de segurança, n.5, set. 2015. Disponível em: <https://www.rnp.br/sites/default/files/media/cais-resumo_mai-agosto-2015.pdf>. Acesso em: 13 fev. 2018.

_____. Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC. Rede Nacional de Ensino e Pesquisa - RNP. **Cais em Resumo**: alertas, vulnerabilidades e incidentes de segurança, n.6, 1º semestre de 2017. Disponível em: <https://www.rnp.br/sites/default/files/06_caisemresumo_ago_rb.pdf>. Acesso em: 13 fev. 2018.

_____. Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC. Rede Nacional de Ensino e Pesquisa - RNP. **Relatório Anual**: Incidentes de segurança da Informação 2013. Brasília, 2013. Disponível em: <https://www.rnp.br/sites/default/files/relatorio_incidentes_2013.pdf>. Acesso em: 13 fev. 2018.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BROCKHOFF, Sarah; KRIEGER, Tim; MEIERRIEKS, Daniel. Heterogeneous Terrorism: Determinants of Left Wing and Nationalist-Separatist Terrorism in Western Europe. **Peace Econ Peace Sci Publ Pol**, 22(4), p. 393–401, 2016.

CALAZANS, Angélica Toffano Seidel. Conceitos e uso da informação organizacional e informação estratégica. **TransInformação**, Campinas, 18, 1, p. 63-70, jan./abr., 2006.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Segurança para Internet, versão 4.0**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>>. Acesso em: 07 set. 2017.

_____. **Estatísticas mantidas pelo CERT.br**. 2016. Disponível em: <<https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>>. Acesso em: 07 set. 2017.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede do ano de 2016**. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2016/Estatisticas_CTIR_Gov_Ano_2016.pdf>. Acesso em: 08 set. 2017.

CHOO, Chun Wei. **A Organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. 3 ed. São Paulo: Senac, 2003.

CHU, Hai-Cheng *et al.* Potential cyberterrorism via a multimedia smart phone based on a web 2.0 application via ubiquitous Wi-Fi access points and the corresponding digital forensics. **Multimedia Systems** , 17, p. 341–349, 2011.

DESLANDES, Suely Ferreira; GOMES, Romeu; MINAYO, Maria Cecília de Souza. **Pesquisa Social**: teoria, método e criatividade. 28. ed. Petrópolis, RJ: Vozes, 2009.

FERNANDES, Jorge Henrique Cabral; SOUZA, Raul Carvalho de. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Studies**: Research Trends, p. 63-75, 2016.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação**: guia prático para elaboração e implementação. 2 ed. Rio de Janeiro: Ciência Moderna, 2008.

FERREIRA, Marcos Alan S. V. **Combate ao terrorismo na América do Sul**: uma análise comparada das políticas do Brasil e dos Estados Unidos para a Tríplice Fronteira. 1. ed. Curitiba: Prismas, 2016.

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

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FLORES, Natália Martins; GOMES, Isaltina Maria de Azevedo Melo. #OcupeEstelita: ciberativismo e mobilização social. **C&S** – São Bernardo do Campo, v. 39, n. 1, p. 219-251, jan./abr. 2017.

GAZETA DO POVO. **Mundo presencia ataque hacker em escala global e serviços públicos são afetados**. 2017. Disponível em: <<http://www.gazetadopovo.com.br/economia/nova-economia/mundo-presencia-ataque-hacker-em-escala-global-e-servicos-publicos-sao-afetados-dhqu9rpm8mb7lf9sw44p6o9we>>. Acesso em: 08 set. 2017.

GODET, Michel. The Art of Scenarios and Strategic Planning: Tools and Pitfalls. **Technological Forecasting and Social Change**, 65, p. 3–22, 2000.

GODET, Michel; DURANCE, Philippe. **A prospectiva estratégica para as empresas e os territórios**. UNESCO, 2011.

GOMES JR., Jonas da Silva. Ativismo ambiental na Web: análise das estratégias de ciberativismo do twitter da WWF-Brasil. **Razón y Palabra: Ingeniería en Comunicación Social**, n. 90, p. 563-579, jun./ago. 2015.

GORDON, Sarah; FORD, Richard. Cyberterrorism? **Computers & Security**, v. 21, n. 7, p. 636-647, 2002.

GORDON, Theodore; SHARAN, Yair; FLORESCU, Elizabeth. Prospects for Lone Wolf and SIMAD terrorism. **Technological Forecasting & Social Change**, 95, p. 234–251, 2015.

HARRIES, David; YELLOWLEES, Peter M. Brief Communication Cyberterrorism: Is the U.S. Healthcare System Safe? **Mary ann Liebert, inc.** Vol. 19, No. 1, p. 61-66, 2013.

HONG, Kwo-Shing *et al.* An integrated system theory of information security management. **Information Management & Computer Security**, p. 243-248, 2003.

HORGAN, John G. Psychology of Terrorism: Introduction to the Special Issue. **American Psychologist**, Vol. 72, No. 3, p. 199–204, 2017.

HUA, Jian; BAPNA, Sanjay. How Can We Deter Cyber Terrorism? **Information Security Journal: A Global Perspective**, 21, p. 102–114, 2012.

HUA, Jian; BAPNA, Sanjay. The economic impact of cyber terrorism. **Journal of Strategic Information Systems**, 22, p.175–186, 2013.

JARVIS, Lee; MACDONALD, Stuart; NOURI, Lella. The Cyberterrorism Threat: Findings from a Survey of Researchers. **Studies in Conflict & Terrorism**, 37, p. 68–90, 2014.

KIM, Eyoung B. Recommendations for information security awareness training for college students. **Information Management & Computer Security**, vol. 22 nº 1, pp. 115-126, 2014.

KONTSELIDZE, Achiko. Cyberterrorism – when technology became a weapon. **European Scientific Journal**, p. 24-29, 2015.

LÁZARO, Alicia Chicharro. La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas. **IDP**, n. 9, p. 1-14, 2009.

LÉVY, Pierre. **Cibercultura**. São Paulo: 34, 1999.

LÉVY, Pierre. **Ciberdemocracia**. Lisboa: Instituto Piaget, 2003.

LIMA, Gabriela Bezerra. Tipos de Ativismo Digital e Ativismo Preguiçoso no Mapa Cultural. **Revista GEMInIS**, V. 3, n. 1, p.71–96, 2012.

MANOEL, Sergio da Silva. **Governança de segurança da informação**: como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 7. ed. São Paulo: Atlas, 2010.

MARTINS, Gilberto de Andrade. **Estudo de caso**: uma estratégia de pesquisa. 2. ed. São Paulo: Atlas, 2008.

MARZOCHI, Samira Feldman. O “ANIMAL ELETRÔNICO”: dilemas do ciberativismo verde. **Caderno CRH**, Salvador, v. 28, n. 73, p. 127-145, Jan./Abr. 2015.

MICHEL, Maria Helena. **Metodologia e pesquisa científica em ciências sociais**. 2.ed. São Paulo: Atlas, 2009.

MINAYO, M. C. S. **O Desafio do conhecimento: pesquisa qualitativa em Saúde**. 11. ed. São Paulo: Hucitec, 2008.

MONTARDO, Sandra Portella; ARAÚJO, Willian. Performance e práticas de consumo *online*: ciberativismo em *sites* de redes sociais. **Revista FAMECOS**, Porto Alegre, v. 20, n. 2, p. 472-494, maio/ago. 2013.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. As dobras semióticas do ciberespaço: da *web* visível à invisível. **TransInformação**, Campinas, 25(1), p. 35-46, jan./abr., 2013.

MORAES, Heloisa Juncklaus Preis. Inteligência coletiva: o ciberespaço como retrato da sociedade ou uma discussão da ética da estética. **Famecos**, Porto Alegre, v. 18, n. 2, p. 542-556, maio/ago. 2011.

MORITZ, Gilberto de Oliveira; NUNER, Rogério; PEREIRA, Maurício Fernandes. Os métodos de prospecção de cenários e sua aplicação nas organizações: um estudo de caso no período 1998-2008. **FACES R. Adm.** Belo Horizonte, v. 7, n. 2, p. 68-83, abr./jun. 2008.

MORITZ, Gilberto de Oliveira; PEREIRA, Maurício Fernandes. Planejamento de cenários: a evolução do pensamento prospectivo. **Revista de Ciências da Administração**, v.7, n.13, p. 1-20, 2005.

MOTA, Bárbara Maria Farias; FIGUEIREDO FILHO, Dalson Britto. Quem controla a política de ninguém? Anonymous Brasil e o ativismo hacker nas redes de comunicação. **Emancipação**, Ponta Grossa, 15, 2, p. 299-315, 2015.

NEVES, Bráulio de Britto. Prefiguração de contrapúblicos em Brad – Uma noite mais nas barricadas. **Revista Galáxia**, São Paulo, n. 20, p. 134-145, dez. 2010.

OLIVEIRA, Cristiano Lessa de. Um Apanhado teórico-conceitual sobre a pesquisa qualitativa: tipos, técnicas e características. **Revista Travessias**, Cascavel, v. 2, n. 3, 2008.

PIZZANI, Luciana et al. A arte da pesquisa bibliográfica na busca do conhecimento. **Rev. Dig. Bibl. Ci. Inf.**, Campinas, v.10, n.1, p.53-66, jul./dez. 2012.

PWC. **Inovando e Transformando em Segurança Cibernética**: Principais conclusões da Pesquisa Global de Segurança da Informação 2016. PWCBrasil, 2016. Disponível em <https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf>. Acesso em: 13 fev. 2018.

_____. **Uma defesa ultrapassada**: Principais resultados da Pesquisa Global de Segurança da Informação 2014 – The Global State of Information Security Survey 2014. PWCBrasil, 2014. Disponível em: <https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 13 fev. 2018.

RODRIGUEZ, Martius Vicente Rodriguez y; SILVA, Thássia Diniz da. Gestão da mudança: implantando a segurança da informação numa organização. **Sustainable Business International Journal**, n. 35, p. 1-30, fev. 2014.

SANDOVAL-ALMAZAN, Rodrigo; GIL-GARCIA, J. Ramon. Towards cyberactivism 2.0? Understanding the use of social media and other information technologies for political activism and social movements. **Government Information Quarterly**, 31, p. 365–378, 2014.

SANTOS, Márcio de Miranda *et al.* Prospecção de tecnologias de futuro: métodos, técnicas e abordagens. In: CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS. **Parcerias Estratégicas**, n. 19. Brasília: CGEE, p. 189 – 229, 2004.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva. Livro Digital. 2 ed. Rio de Janeiro: Elsevier, 2014.

SILVA, Narjara Bárbara Xavier; ARAÚJO, Wagner Junqueira de; AZEVEDO, Patrícia Moraes de. Engenharia social nas redes sociais *online*: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **RICI: R.Ibero-amer. Ci. Inf.**, Brasília, v. 6, n. 2, p. 37-55, ago./dez. 2013.

SINGH, Arun Kumar *et al.* Vulnerabilities of Electronics Communication: solution mechanism through script. **International Journal of Computer Science Issues**,

Vol. 8, Issue 3, No. 1, p. 572-582, May 2011.

SOUZA, Carlos Henrique Medeiros de; COSTA, Marco Aurélio Borges. Fronteiras do ciberespaço. **Vértices**, v. 7, n. 1/3, p. 105-114, jan./dez. 2005.

SPUTNIK. **Capacidade inimaginável: hackers norte-coreanos esperam ordem para destruir Coreia do Sul**. 2017. Disponível em: <https://br.sputniknews.com/asia_oceania/201710139577030-hackers-norte-coreanos-esperam-ordem-para-destruir-coreia-do-sul/>. Acesso em: 13 out. 2017.

TEHRANI, Pardis Moslemzadeh; MANAP, Nazura Abdul; TAJI, Hossein. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. **Computer Law & Security Review**, 29, p. 207-215, 2013.

VEJA. **'Multinacional' do cibercrime é responsável por ataque hacker**. 2017. Disponível em: <<http://veja.abril.com.br/mundo/multinacional-do-cibercrime-e-responsavel-por-ataque-hacker/>>. Acesso em: 12 out. 2017.

VEJA. **PF prende grupo que preparava ataques terroristas no Brasil**. 2016a. Disponível em: <<http://veja.abril.com.br/brasil/pf-prende-grupo-que-preparava-atos-de-terrorismo-no-brasil-diz-fonte-do-ministerio-da-justica/>>. Acesso em: 08 set. 2017.

VEJA. **Terrorista mata um policial e sua mulher em ataque na França**. 2016b. Disponível em: <<http://veja.abril.com.br/mundo/terrorista-mata-um-policial-e-sua-mulher-em-ataque-na-franca/>>. Acesso em: 16 ago. 2017.

VENTURA, Magda Maria. O estudo de caso como modalidade de pesquisa. **Rev SOCERJ**. v. 20, n. 5, p. 383-386, 2007.

VLAVO, Fidele. Framing digital activism: The spectre of cyberterrorism. **First Monday**, v. 20, n. 10 – 5, out. 2015.

WRIGHT, James Terence Coulter; SILVA, Antonio Thiago Benedete; SPERS, Renata Giovinazzo. Prospecção de cenários: uma abordagem plural para o futuro do Brasil em 2020. **Revista Ibero-Americana de Estratégia - RIAE**, São Paulo, v. 9, n. 1, p. 56-76, jan./abr. 2010.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. 3. ed. Porto Alegre: Bookman, 2005.

ZANON, Sandra Buth. Gestão e segurança da informação eletrônica: Exigências para uma gestão documental eficaz no Brasil. **Biblios**, n. 56, p. 69-79, 2014.

APÊNDICE A – Termo de Consentimento Livre e Esclarecido (TCLE)

Prezado(a) Sr(a):

A pesquisa intitulada “**Ciber terrorismo na Paraíba: um estudo prospectivo**”, desenvolvida por mim, mestrando José Roberto Cavalcante da Silva, Matrícula 20161019498, sob a orientação do Prof. Dr. Wagner Junqueira de Araújo do Programa de Pós-Graduação em Gestão em Organizações Aprendentes (PPGOA) do Centro de Educação (CE) – Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba (UFPB)-CAMPUS I. Ela tem como objetivo geral **estudar cenários prospectivos sobre o ciber terrorismo na Paraíba**, e como objetivos específicos:

- Identificar as variáveis-chave e os atores do ciber terrorismo em organizações públicas ou privadas da Paraíba;
- Examinar a interação das variáveis e dos atores;
- Elaborar cenários prospectivos para o ciber terrorismo na Paraíba por meio do uso do método de construção de cenários prospectivos de Michel Godet;
- Propor ações para gestão da segurança da informação nos cenários desenvolvidos.

A finalidade deste trabalho é contribuir para criar mecanismos de proteção que reduza a atuação do ciber terrorismo sob a informação de organizações públicas ou privadas, bem como subsidiar a tomada de decisão estratégica da área de gestão da segurança da informação, no sentido de promover modelos para defesa adequada contra o ciber terrorismo.

Para concretizar minha pesquisa, solicito a colaboração e participação do Sr(a). neste formulário (questionário) de coleta de dados, bem como a sua autorização para apresentar os resultados deste estudo em eventos da área de Ciências humanas e Sociais e a publicação em periódicos científicos e/ou na forma de livro impresso ou digital (se for o caso). Saliento, por sua vez, que a sua participação não infligirá e nem trará nenhum dano à sua saúde física ou psíquica, visto que não se trata de uma pesquisa que envolva experimentos da área da saúde. Além disso, o sigilo será estabelecido no sentido de resguardar o anonimato e a não identificação do Sr. (a) enquanto participante desse trabalho ao mostrar sua percepção durante a resolução do formulário (questionário). Esclareço, por outro lado, que sua participação no estudo é voluntária e, sendo assim, o (a) Sr.(a) tem plena liberdade de recusar a participar ou retirar o seu consentimento em qualquer fase da pesquisa sem penalização alguma. Assim, informamos que esta pesquisa não oferece riscos previsíveis para a sua saúde física ou psíquica

Diante do exposto, ao assinar este Termo de Consentimento Livre e Esclarecido (TCLE), o Sr.(a) declara-se devidamente esclarecido (a) e dá o seu consentimento para participar da pesquisa, bem como para a publicação dos resultados obtidos. E para que o referido Termo se constitua em um instrumento de pactuação entre o pesquisador e o (a) Sr. (a) o sujeito da pesquisa, solicito, por gentileza, que rubrique todas as folhas desse Termo de Consentimento Livre e Esclarecido (TCLE), acrescentando sua assinatura na última página.

Ademais, o Sr. (a) receberá uma cópia desse Termo no qual constam o telefone e o endereço do pesquisador responsável, bem como o endereço e telefones do Comitê de Ética – UFPB/CAMPUS I para a qualquer momento queira entrar em contato.

Atenciosamente,

Mestrando José Roberto Cavalcante da Silva/Pesquisador Responsável

Assinatura do Participante da Pesquisa

Contatos telefônicos e e-mail:

Pesquisador(a) Responsável:

(83) 99858-0476 - Endereço do(a) Pesquisador(a) Responsável: Rua Malaquias Timótheo de Souza, Nº98, casa 102 – Bairro Cuiá – João Pessoa-PB - CEP: 58.077-186 / e-mail: cavalcant roberto10@gmail.com

Comitê de Ética da UFPB:

E-mail: eticaccsufpb@hotmail.com/ eticaccs@ccs.ufpb.br

Endereço: UNIVERSITARIO S/N

Bairro: CASTELO BRANCO

Telefone: (83)3216-7791

Fax: (83)3216-7791

UF: PB **Município:** JOAO PESSOA

CEP: 58.051-900

APÊNDICE B – Formulário para a Coleta de Dados

Formulário para o estudo prospectivo sobre o Ciber Terrorismo na Paraíba

Este formulário é aplicado para verificar as variáveis, os atores e as influências entre as variáveis e os atores do Ciber terrorismo na Paraíba. Ressalta-se que esta pesquisa não oferece risco ao participante nem à sua instituição, apresentando um caráter confidencial, ficando resguardado o nome do participante e de sua instituição. O formulário apresenta questões gerais acerca de ataques cibernéticos e sobre a segurança da informação que podem ser aplicadas a qualquer instituição pública ou privada. Além disso, traz questionamentos acerca do grau de influências de variáveis apontadas no levantamento bibliográfico de nosso projeto de pesquisa, que são fundamentais para a construção de cenários prospectivos do Ciber terrorismo na Paraíba. **Diante do exposto, solicita-se a sua colaboração no sentido de responder as questões deste formulário?**

Sobre a situação da segurança da informação das organizações contemporâneas	
1) As organizações contemporâneas necessitam de Gestão de Segurança da Informação no ciberespaço?	☐ Discordo totalmente ☐ Discordo parcialmente ☐ Não concordo, nem discordo ☐ Concordo parcialmente ☐ Concordo totalmente
2) A sua organização está preparada para assegurar os princípios básicos da segurança da informação no atual contexto de avanço tecnológico?	☐ Discordo totalmente ☐ Discordo parcialmente ☐ Não concordo, nem discordo ☐ Concordo parcialmente ☐ Concordo totalmente
3) Existe uma política de segurança da informação em sua organização?	☐ Discordo totalmente ☐ Discordo parcialmente ☐ Não concordo, nem discordo ☐ Concordo parcialmente ☐ Concordo totalmente
Sobre as ameaças à segurança da informação das organizações contemporâneas	
4) A ausência de uma definição clara acerca das ameaças prejudica	☐ Discordo totalmente ☐ Discordo parcialmente ☐ Não concordo, nem discordo ☐ Concordo parcialmente

a segurança da informação das organizações contemporâneas?	☐ Concordo totalmente
5) A maioria dos ataques cibernéticos ocorre pelo fato de existir uma estreita relação entre tecnologias, processos e pessoas?	☐ Discordo totalmente ☐ Discordo parcialmente ☐ Não concordo, nem discordo ☐ Concordo parcialmente ☐ Concordo totalmente
6) Coloque em ordem a ameaça à segurança da informação mais recorrente nas organizações contemporâneas?	Naturais () Involuntárias () Voluntárias ()
Sobre o fenômeno Ciber terrorismo	
7) Você conhece organizações contemporâneas que sofreram ataques de natureza Ciber terrorista?	☐ Sim ☐ Não ☐ Comente () se foi em João Pessoa – se foi fora.....
8) Coloque em ordem a motivação de um ataque de natureza Ciber terrorista?	Política () Social () Ideológica () Financeira ()
Sobre medidas de proteção e combate contra as ameaças virtuais como o Ciber terrorismo	
9) Coloque em ordem as medidas de segurança contra o Ciber terrorismo?	Contínuas atualizações de sistema, softwares e aplicativos () Treinamentos de pessoal () Processos organizacionais estabelecidos () Termos e documentação organizacionais que responsabilizem os colaboradores () Legislação ()
10) Cite outras medidas de prevenção e/ou combate ao Ciber terrorismo?	

Para auxiliar nossa pesquisa, necessita-se verificar sua percepção sobre a influência/dependência dos elementos contidos nas tabelas abaixo. Eles foram identificados em nossa pesquisa mediante levantamento bibliográfico como fundamentais para a construção dos cenários do Ciber terrorismo na Paraíba. Com base em suas opiniões e experiências sobre Segurança da Informação no contexto organizacional, poderia apontar nos quadros a seguir:

11) Grau de influência direta que uma variável exerce sobre a outra?

	Políticas Públicas	Ideologias	Mercado	Tecnologias	Vantagem Indevida
Políticas Públicas	0				
Ideologias		0			
Mercado			0		
Tecnologias				0	
Vantagem Indevida					0

Legenda: Grau de influência de uma variável sobre a outra: **(0) Sem Influência Direta; (1) Fraca; (2) Média; (3) Forte; e (P) Potenciais** (podem ocorrer em algum momento no futuro).

12) Grau de influência que um ator exerce sobre o outro?

	Governo	Empresas	Colaboradores	Clientes/Usuários	Pessoas Externas
Governo	0				
Empresas		0			
Colaboradores			0		
Clientes/Usuários				0	
Pessoas Externas					0

Legenda: Grau de influência de um ator sobre o outro em relação ao/à: **(0) Sem Influência Direta; (1) Processos; (2) Projetos; (3) Missão; e (4) Existência.**

13) O grau de relevância do objetivo/desafio em relação aos atores?
--

	Elaborar Políticas Públicas	Divulgar Ideologias	Novas Ideias	Uso das Tecnologias	Benefícios Ilícitos
Governo					
Empresas					
Colaboradores					
Clientes/Usuários					
Pessoas Externas					

Legenda: O objetivo tem consequência em relação ao ator sobre seu/sua: o sinal (+/-) indica se o ator é favorável ou desfavorável ao objetivo; (0) o objetivo é pouco consequente; (1) o objetivo tem consequências sobre os processos do ator/ é indispensável para o bom funcionamento dos processos operacionais, de gestão, etc.; (2) o objetivo tem consequências sobre os projetos do ator/ é indispensável para a realização de seus projetos; (3) o objetivo tem consequências sobre a missão do ator/ é indispensável para o cumprimento de sua missão; (4) o objetivo tem consequências sobre a existência do ator/ é indispensável para a sua perenidade.

Obrigado por sua colaboração!!!

ANEXO A – PARECER CONSUBSTANCIADO DO COMITÊ DE ÉTICA

UFPB - CENTRO DE CIÊNCIAS
DA SAÚDE DA UNIVERSIDADE
FEDERAL DA PARAÍBA



PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: CIBER TERRORISMO NA PARAÍBA: UM ESTUDO PROSPECTIVO

Pesquisador: JOSE ROBERTO CAVALCANTE DA SILVA

Área Temática:

Versão: 2

CAAE: 80482617.6.0000.5168

Instituição Proponente: Universidade Federal da Paraíba

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 2.509.426

Apresentação do Projeto:

Trata-se de um projeto de pesquisa egresso do MESTRADO PROFISSIONAL EM GESTÃO EM ORGANIZAÇÕES APRENDENTES, do CENTRO DE EDUCAÇÃO, da UNIVERSIDADE FEDERAL DA PARAÍBA, do aluno JOSE ROBERTO CAVALCANTE DA SILVA, sob orientação do professor Dr^a. Prof. Dr. Wagner Junqueira de Araújo.

Objetivo da Pesquisa:

Objetivo Geral:

Estudar cenários prospectivos sobre o ciber terrorismo na Paraíba.

Objetivos Específicos:

- a) Identificar as variáveis-chave e os atores do ciber terrorismo em organizações públicas ou privadas da Paraíba;
- b) Examinar a interação das variáveis e dos atores;
- c) Elaborar três cenários prospectivos para o ciber terrorismo na Paraíba por meio do uso do método de construção de cenários prospectivos de Michel Godet;
- d) Propor ações para gestão da segurança da informação nos cenários desenvolvidos.

Endereço: UNIVERSITÁRIO S/N

Bairro: CASTELO BRANCO

CEP: 58.051-900

UF: PB

Município: JOÃO PESSOA

Telefone: (83)3216-7791

Fax: (83)3216-7791

E-mail: eticaccsu@ufpb@hotmail.com

UFPB - CENTRO DE CIÊNCIAS
DA SAÚDE DA UNIVERSIDADE
FEDERAL DA PARAÍBA



Continuação do Parecer 2.508.428

Avaliação dos Riscos e Benefícios:

Riscos:

Os riscos para os participantes serão mínimos, uma vez que a presente pesquisa envolve apenas a coleta de dados através de formulário, além dos pesquisadores garantirem sigilo de identidade e imagem.

Benefícios:

A pesquisa auxiliará a tomada de decisão dos gestores de segurança da informação a partir da criação dos cenários futuros sobre o terrorismo cibernético.

Comentários e Considerações sobre a Pesquisa:

O presente projeto apresenta coerência científica, mostrando relevância para a academia, haja vista a ampliação do conhecimento, onde se busca, principalmente, Estudar cenários prospectivos sobre o ciberterrorismo na Paraíba.

Considerações sobre os Termos de apresentação obrigatória:

Todos os Termos de Apresentação Obrigatória foram anexados tempestivamente.

Recomendações:

RECOMENDAMOS QUE AO TÉRMINO DA PESQUISA, O PESQUISADOR RESPONSÁVEL ENCAMINHE AO COMITÊ DE ÉTICA EM PESQUISA DO CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA, RELATÓRIO FINAL, DOCUMENTO DEVOLUTIVO COMPROVANDO QUE OS DADOS FORAM DIVULGADOS JUNTO À INSTITUIÇÃO ONDE OS MESMOS FORAM COLETADOS E A PESQUISA NA ÍNTEGRA, TODOS EM PDF, VIA PLATAFORMA BRASIL, ATRAVÉS DE NOTIFICAÇÃO, PARA OBTENÇÃO DA CERTIDÃO DEFINITIVA.

Conclusões ou Pendências e Lista de Inadequações:

Tendo em vista o cumprimento das pendências elencadas anteriormente, SOMOS DE PARECER FAVORÁVEL A EXECUÇÃO DO PRESENTE PROJETO, DA FORMA COMO SE APRESENTA.

Considerações Finais a critério do CEP:

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou a execução do referido projeto de pesquisa.

Outrossim, informo que a autorização para posterior publicação fica condicionada à submissão do Relatório Final na Plataforma Brasil, via Notificação, para fins de apreciação e aprovação por este

Endereço: UNIVERSITÁRIO S/N

Bairro: CASTELO BRANCO

CEP: 58.051-900

UF: PB

Município: JOÃO PESSOA

Telefone: (83)3216-7791

Fax: (83)3216-7791

E-mail: eticaccsu@pb@hotmail.com

**UFPB - CENTRO DE CIÊNCIAS
DA SAÚDE DA UNIVERSIDADE
FEDERAL DA PARAÍBA**



Continuação do Parecer: 2.509.426

egregio Comitê.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BASICAS_DO_PROJETO_1039188.pdf	01/02/2018 12:42:42		Aceito
Outros	Declaracao_qualificacao.pdf	01/02/2018 12:41:51	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Outros	Apendice_B_Formulario_pesquisa_Ciberterrorismo.pdf	01/02/2018 12:40:53	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Apendice_A_TCLE.pdf	01/02/2018 12:39:16	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Outros	CRONOGRAMA_ATIVIDADES.pdf	01/02/2018 12:39:01	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_UEPB.pdf	01/02/2018 12:33:19	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_TJPB.pdf	01/02/2018 12:32:44	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_STI_UFPB.pdf	01/02/2018 12:31:46	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_IFPB_Reitoria.pdf	01/02/2018 12:31:29	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_IFPB_Campus_Joao_Pessoa.pdf	01/02/2018 12:31:06	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	Termo_Anuencia_Codata.pdf	01/02/2018 12:30:44	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Projeto Detalhado / Brochura Investigador	Projeto_Pesquisa_Detalhado.pdf	01/02/2018 12:30:17	JOSE ROBERTO CAVALCANTE DA SILVA	Aceito
Folha de Rosto	Folha_Rosto.pdf	28/11/2017	JOSE ROBERTO	Aceito

Endereço: UNIVERSITÁRIO S/N

Bairro: CASTELO BRANCO

CEP: 58.051-900

UF: PB

Município: JOÃO PESSOA

Telefone: (83)3216-7791

Fax: (83)3216-7791

E-mail: etica@ccsu.pb@gmail.com

UFPB - CENTRO DE CIÊNCIAS
DA SAÚDE DA UNIVERSIDADE
FEDERAL DA PARAÍBA



Continuação do Parecer: 2.539.426

Folha de Rosto	Folha_Rosto.pdf	17:31:54	CAVALCANTE DA SILVA	Aceito
----------------	-----------------	----------	------------------------	--------

Situação do Parecer:

Aprovado

Necessita Apreciação da CONEP:

Não

JOAO PESSOA, 23 de Fevereiro de 2018

Assinado por:

Elaine Marques Duarte de Sousa
(Coordenador)

Endereço: UNIVERSITARIO S/N

Bairro: CASTELO BRANCO

CEP: 58.051-900

UF: PB

Município: JOAO PESSOA

Telefone: (83)3216-7791

Fax: (83)3216-7791

E-mail: etloccsu@ufpb@hotmail.com