UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Eduardo Wallier Vianna

ANÁLISE DO COMPORTAMENTO INFORMACIONAL NA GESTÃO DA SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Brasília – DF
2015

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Eduardo Wallier Vianna

ANÁLISE DO COMPORTAMENTO INFORMACIONAL NA GESTÃO DA SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Dissertação apresentada ao programa de Pós-graduação em Ciência da Informação da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Ciência da Informação

Orientador: Prof. Dr. Jorge Henrique Cabral Fernandes

Brasília – DF
2015

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1019892.

Vianna, Eduardo Wallier.
V617a Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal / Eduardo Wallier Vianna. -- 2015.
115 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Faculdade de Ciência da Informação, Programa de Pós-Graduação em Ciência da Informação, 2015.
Inclui bibliografia.
Orientação: Jorge Henrique Cabral Fernandes.

1. Administração pública. 2. Comportamento informacional. 3. Segurança da informação. I. Fernandes, Jorge Henrique Cabral. II. Título.

CDU 002:004

FOLHA DE APROVAÇÃO

Título: "Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal".

Autor (a): Eduardo Wallier Vianna

Área de concentração: Gestão da informação

Linha de pesquisa: Organização da Informação

Dissertação submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-graduação em Ciência da Informação da Faculdade em Ciência da Informação da Universidade de Brasília como requisito parcial para obtenção do título de **Mestre** em Ciência da Informação.

Dissertação aprovada em: 22 de Janeiro de 2015.

Prof. Dr. Jorge Henrique Cabral Fernandes
Presidente (UnB/PPGCINF)

Prof. Dr. Renato Tarciso Barbosa de Sousa
Membro Interno (UnB/PPGCINF)

Prof. Dr. Felipe Lopes da Cruz
Membro Externo (DPF/MJ)

Prof. Dr. Rogério Henrique de Araujo Junior
Suplente - (UnB/PPGCINF)

A MINHA FAMÍLIA QUERIDA,

razão do meu viver.

.

AGRADECIMENTOS

Às secretárias do PPGCINF Martha e Jacqueline
pela colaboração e solicitude.

Às professoras*:*
Maria de Lourdes Barbosa Vianna e
Sely Maria de Souza Costa
pela especial atenção e compartilhamento generoso dos seus conhecimentos.

As *colegas do PPGCInf:*
Anna Maria, Helena Sacerdote e Sonia Boeres
pela amizade e apoio imprescindíveis na realização dessa pesquisa.

Ao meu *Orientador, Professor Doutor Jorge Henrique Cabral Fernandes*
pelos conhecimentos e experiências transmitidas e pelo apoio em tempo oportuno.

Aos *meus pais Regina Wallier Vianna e Bento Barbosa Vianna*,
pelas lições de vida que me transmitem e pelos exemplos de superação e determinação na busca das aspirações.

A *minha família querida:*
Mônica, Aninha e Carlinhos,
razão do meu viver, fonte de carinho e inspiração
pelo amor incondicional.

Ao *nosso DEUS,*
por tudo.

Muito obrigado!

A fé é o combustível da vida.
Leo Tolstoi

Quem sabe tropeçar não cai.
Ditado alemão

RESUMO

Este estudo analisa as necessidades informacionais dos profissionais que atuam na gestão da segurança do espaço cibernético, no âmbito da Administração Pública Federal (APF). A pesquisa considera que a Ciência da Informação (CI) envolve o estudo da informação, sua interação com as Tecnologias de Informação e Comunicações (TIC) e o relacionamento referente à segurança da informação. Ressalta, inclusive, que a segurança cibernética ou do espaço cibernético encontra-se inserida no contexto mais amplo e multifacetado da segurança da informação. A pesquisa identifica as fontes, os canais e os usos da informação, buscando mapear o comportamento informacional de um grupo representante de agentes públicos, quando envolvidos na segurança cibernética na APF. Possui, como contexto de análise, os concludentes e alunos do Curso de Especialização em Gestão da Segurança da Informação e Comunicações (CEGSIC), realizado pela Universidade de Brasília, por demanda do Gabinete de Segurança Institucional da Presidência da República (GSIPR). A análise é realizada de forma mista sequencial em duas fases. Na primeira, ocorre a realização de um levantamento amplo para generalizar os resultados por meio da aplicação de um questionário. Na segunda fase, após a análise dos dados quantitativos levantados (fontes e canais de informação mais relevantes, acessíveis e confiáveis; e usos da informação mais frequentes e pertinentes), são realizadas entrevistas, a fim de se obter uma visão detalhada das peculiaridades do comportamento informacional. Foi identificado que as necessidades de informação estão relacionadas primariamente com a perspectiva de atuação em nível estratégico (coordenação, planejamento e gestão de alto nível). Os resultados indicaram um equilíbrio na relevância entre a utilização de fontes internas e externas à organização, independentemente de serem pessoais ou não. Além disso, o uso da informação aponta atividades centradas na aprendizagem individual para o aprimoramento da segurança organizacional. Mais à frente, espera-se que os resultados obtidos com a presente pesquisa contribuam para a melhoria dos níveis de segurança cibernética nas organizações.

Palavras-chave: Necessidades de Informação. Comportamento Informacional. Segurança Cibernética. Segurança da informação. Administração Pública Federal.

ABSTRACT

This study analyze the informational necessities of the professionals witch act on the management of the security of the cyber space, on the framework of Federal Public Administration (FPA). The research finds that the Science Information (CI) involves the study of information, its interaction with the Information and Communications Technologies (ICT) and the relationship related to information security. Points out, that even cyber security or cyber space is inserted in the broadest and multifaceted context of security information. The research identifies the sources, channels and the uses of information, seeking to map the information behavior of a representative group of officials, when involved in cyber security in the FPA. It has, as context analysis, the graduated and students of the Course of Specialization in Management of Security Information and Communications (CEGSIC), conducted by the University of Brasilia, on demand of the Cabinet of Institutional Security of the Presidency of Republic (GSIPR). The analysis is performed in sequentially mixed form in two phases. In the first, occurs the execution of a broad survey to generalize the results through the application of a questionnaire. In the second phase, after the analysis of the quantitative data collected (most relevant information channels and sources, affordable and reliable, and uses of the information more frequent and relevant), interviews are conducted in order to obtain a detailed view of the peculiarities of informational behavioral. It was identified that the information needs are related primarily to the perspective of action at the strategic level (coordination, planning and high level management). The results indicated equilibrium in the relevance between the use of sources internal and external to the organization, regardless of being personal or not. In addition, the use of information points to activities focused on individual learning for the improvement of organizational security. Further ahead, it is expected that the results of this research contribute to the improvement of cyber security levels in organizations.

Keywords: Information Needs. Informational behavior. Cybersecurity. Information security. Federal Public Administration.

.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Considerações iniciais

O governo brasileiro, à semelhança das demais grandes e modernas nações, utiliza, em larga escala, as mais diversas possibilidades dos sistemas de informação automatizados e de redes de comunicação de dados. Nesse sentido, o governo vem disponibilizando aos cidadãos um crescente acervo de páginas, documentos, dados, aplicações e serviços *on-line*, interligados por meio da rede mundial de computadores - Internet (NIC.br, 2010).

De acordo com o investigado no Senado Federal (2014), o Brasil é o terceiro país do mundo em números de usuários ativos de Internet. Além disso, verificou-se um crescimento significativo do número de organizações governamentais que disponibilizam serviços na Internet, passando o percentual de 49%, em 2012, para 88%, em 2014 (BRASIL, 2014).

A Administração Pública Federal (APF), também conhecida como Poder Executivo ou Federal, possui grande número de entidades, uma complexa hierarquia, diferenças orçamentárias, na qualificação de pessoal, nas práticas e políticas já estabelecidas, bem como nos níveis de segurança implementados. Dessa forma, na abordagem de "governo eletrônico" (e-gov), a APF, a fim de apoiar as mais diversificadas ações governamentais, vem adotando soluções multifacetadas, fortemente suportadas nas tecnologias de informação (TI), inseridas no contexto do espaço cibernético. Segundo a ISO/IEC 27032 (2012, tradução nossa), espaço cibernético é entendido como "um ambiente complexo resultante da interação de pessoas, *software* e serviços existentes na Internet, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física".[1]

A título de exemplo, pode-se citar a Lei 12.527/2011 de Acesso à Informação (LAI) que entrou em vigor em maio de 2012. A LAI estabeleceu que o Estado Brasileiro ofereça acesso rápido e fácil às informações que estão sob sua guarda; e que essas informações devem ser apresentadas de forma clara, objetiva e de fácil entendimento, empregando, sempre que possível, as Tecnologias de Informação e Comunicação (TIC), no caso utilizadas como sinônimo de TI.

---

[1] *Cyberspace - the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.*

Esse conjunto de conteúdos digitais públicos ou de utilização restrita tem sido alvo de ações mal-intencionadas por diferentes grupos com os mais diversos e escusos objetivos[2]. A título de exemplo, o cidadão, no seu cotidiano, toma consciência de parte dessas ações danosas em pelo menos três situações: (1) ao perceber o vazamento de seus dados particulares que estavam sob custódia de um órgão público ou (2) ao descobrir que valores numéricos pessoais, armazenados em uma base de dados governamental, foram alterados sem a aquiescência e conhecimento do responsável pela guarda das informações, ou, ainda, (3) quando não consegue acessar um serviço público porque o sítio do governo está fora do ar.

O exemplo anterior tipifica, respectivamente, (1) rupturas na confidencialidade, (2) comprometimento da integridade e (3) perda da disponibilidade da informação, sob a responsabilidade do e-gov. A despeito de algumas variações e discussões conceituais, essas são as três propriedades (tríade) mais importantes relativas à segurança cibernética, conhecidas pela sigla CID ou CIA (*confidentiality, integrity and availability*). Ou seja, as atividades de segurança cibernética buscam a preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético considerado, bem como de outras propriedades como: autenticidade, responsabilidade, não repúdio e confiabilidade (ISO/IEC 27032, 2012, tradução nossa).[3]

Os Estados nacionais estão inseridos neste cenário de ações adversas, sendo, por conseguinte, reféns dos perigos, riscos e incertezas inerentes ao uso das Tecnologias de Informação e Comunicações, típicos do espaço cibernético. Potencializando as consequências maléficas das ações mal-intencionadas, Freitas; Gomes e Rêgo Barros (2011) afirmam que o espaço cibernético desconhece fronteiras e tem potencial para causar grandes prejuízos financeiros, paralisar as estruturas vitais de uma nação e, até mesmo, indiretamente, ceifar vidas.

Neste contexto, o amplo e heterogêneo ciclo de eventos internacionais sediados pelo Brasil que se iniciaram em 2012 com a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio+20), seguida da Copa das Confederações (Copa Conf 2013), da Jornada Mundial da Juventude (JMJ 2013), da Copa do Mundo de Futebol (FIFA 2014) e se estendem até 2016 com os Jogos Olímpicos e Paralímpicos, de igual forma, vêm contribuindo para evidenciar a importância e a necessidade imprescindível da segurança no espaço cibernético como vetor de sustentabilidade do Estado brasileiro. Destaca-se que a realização dos

---

[2] Como exemplo, podem-se consultar as Estatísticas de tratamento de incidentes nas redes e sistemas da APF, compiladas pelo Centro de Tratamento de Incidentes de Segurança de Redes de Computadores (CTIR Gov). Disponível em: < http://www.ctir.gov.br/estatisticas.html>. Acesso em: 09 jun. 2014.

[3] *Cybersecurity - preservation of confidentiality, integrity and availability of information in the ciberspace. In addition, other properties. such as authenticity, accountability, non-repudiation, and reliability can also be involved.*

chamados "Grandes Eventos" trouxe aspectos diferenciados e inovadores no contexto da segurança do país e, até o presente, contou com a participação de um Destacamento de Defesa Cibernética a cargo do Ministério da Defesa nos planejamentos de emprego e ações operacionais de segurança pública e defesa nacional (WALLIER VIANNA, 2013a).

1.2 Questão da pesquisa

As mudanças no cenário internacional, os avanços dos meios de comunicação da informação e a inovação tecnológica colocam os governos e as instituições públicas com responsabilidades desafiadoras, no que tange à segurança das informações no espaço cibernético, ou seja, aquelas produzidas ou armazenadas nos sistemas de informação automatizados da organização ou que trafegam pelas suas redes internas e pela Internet. Na delimitação do problema da presente pesquisa, considera-se que a segurança dos dados e das informações institucionais envolve não somente o uso das TICs, mas também os processos, o ambiente e as pessoas.

Via de regra, a facilidade de alocação de recursos financeiros e o próprio ambiente tecnológico induzem soluções de segurança baseadas, quase que exclusivamente, em aquisições de equipamentos (*hardware*) ou de aplicativos (*software*) (BRASIL, 2013). Essas soluções são incompletas, pois, no seu cerne, necessitam de **pessoas** qualificadas para responder as falhas ou os incidentes indesejados que possam comprometer a segurança do espaço cibernético da organização. Neste contexto, o agente público que atue nas atividades de segurança cibernética deve possuir competências para, no mínimo:

a) participar do planejamento e da adequação do uso das TICs na sua organização;
b) instalar corretamente o *hardware* adquirido*;*
c) configurar o *software* de acordo com o ambiente computacional e as peculiaridades da sua organização;
d) monitorar e aprimorar o funcionamento das soluções de "negócio" adotadas pela organização e suportadas pela infraestrutura de TIC.

Consequentemente, o exercício da segurança cibernética extrapola o aspecto técnico/operacional e envolve o relacionamento interpessoal, o intercâmbio de informações e a tomada compartilhada de decisões. Tal consideração encontra ressonância em Lima-Marques e Marciano (2006), quando afirmam que o crescimento alarmante dos incidentes relacionados à segurança da informação alerta para a premente necessidade de uma visão fundamentada em bases sólidas para este problema, a qual extrapola em muito o âmbito da tecnologia.

O cenário dinâmico e mutável, devido especialmente à introdução célere de novas tecnologias, ressalta o papel das pessoas que atuam diretamente na gestão da segurança cibernética. Dessa forma, cresce de importância o aprimoramento profissional constante, que se torna pedra angular na redução da insegurança cibernética organizacional.

Como pode ser percebido, o campo de atuação e a gama de competências inerentes às atividades do profissional de segurança cibernética são temas vastos e heterogêneos, demandando conhecimentos gerenciais e técnicos sobre: legislação, normas e regulamentos inerentes à instituição onde atua; formas de ataques e exploração de fragilidades computacionais; sistemas operacionais e arquitetura de computadores; programação e linguagens diversas; redes de computadores e protocolos de comunicação na Internet, dentre outros.

Neste contexto informacional multifacetado e complexo em que está inserido o gestor de segurança cibernética, a presente pesquisa visa responder ao seguinte questionamento: quais são as fontes e os canais que atendem às necessidades informacionais e como acontece o uso da informação de um agente público que atua na gestão da segurança do espaço cibernético institucional no âmbito da Administração Pública Federal?

Cabe destacar que autores e pesquisadores contemporâneos reconhecem a substituição da nomenclatura "necessidades, busca e uso da informação" por comportamento informacional, de forma que o assunto é revisado na subseção 2.4.4.

1.3 Objetivos

1.3.1 Objetivo Geral

Analisar o comportamento informacional dos agentes públicos que atuam na gestão da segurança cibernética governamental, no âmbito da Administração Pública Federal.

1.3.2 Objetivos específicos (OE)

a) identificar as fontes e os canais de informação mais utilizados pelos agentes públicos na gestão da segurança cibernética na Administração Pública Federal;
b) identificar os mais significativos usos da informação pelos agentes públicos, no contexto da segurança em um espaço cibernético numa organização da Administração Pública Federal;

c) mapear o comportamento informacional de um grupo representante de agentes públicos, quando envolvidos na segurança cibernética na Administração Pública Federal.

1.4 Justificativa

A pesquisa foi motivada por observações realizadas pelo autor, em organizações nacionais públicas e privadas que operam na área da segurança e defesa cibernéticas, particularmente naquelas que atuam diretamente na gestão de incidentes em redes de computadores, como o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov), subordinado à Presidência da República (PR), e o Centro de Defesa Cibernética (CDCiber) do Ministério da Defesa (MD).

Não obstante os inquestionáveis benefícios oriundos da evolução experimentada pelas TICs, o espaço cibernético constitui-se como um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações. Esse espaço é caracterizado pela assimetria[4] entre os envolvidos em conflitos, pela dificuldade de atribuição de responsabilidades por ações e pelo paradoxo da maior vulnerabilidade do mais forte (FREITAS; GOMES; RÊGO BARROS, 2011). Paradoxalmente ao inexorável desenvolvimento tecnológico, o ser humano detém papel essencial no controle e na segurança do espaço cibernético (onde, invariavelmente, circula grande parte da informação em tempo real), devendo sua capacidade profissional ser objeto de constante estudo e aperfeiçoamento.

Ao se discutir a segurança da informação e as TIC, como complementares da CI no processo da organização da informação, do conhecimento registrado e da sua assimilação e uso, entende-se que há compatibilidade com a clássica, e ainda atual, definição de Ciência da Informação por Borko (1968):

> é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam seu fluxo e os meios de processamento para otimizar sua acessibilidade e utilização. Relaciona-se com o corpo de conhecimento relativo à produção, coleta, organização, armazenagem, recuperação, interpretação, transmissão, transformação e utilização da informação.

[4] A assimetria entre os envolvidos em um conflito no espaço cibernético decorre da possibilidade de emprego de uma ampla variedade de formas e meios para realizar ações ofensivas contra os recursos de um oponente, inclusive de forma fácil, rápida e barata, quando comparada a uma menor variedade de formas e meios para realizar ações defensivas, com mais dificuldades, lentidão e custos.

Percebe-se, também nesse sentido, alinhamento da segurança da informação com as características ou razões da existência e evolução da CI apresentadas por Saracevic (1996), que são: a natureza interdisciplinar da CI, a ligação inexorável da CI com a tecnologia da informação [suportam os sistemas de informação (SI)] e a participação da CI ativa e deliberada na evolução da sociedade da informação [cada vez mais dependes de SI - que devem estar seguros (CID)]. Fernandes (2010), a fim de situar a segurança da informação no âmago da ciência da informação, recorreu à taxionomia de Zins. O autor argumenta que a Segurança da Informação pode ser um modelo para a CI, tendo em vista que várias facetas do mapa do conhecimento da CI proposto por Zins são claramente articuladas nos modelos de gestão da segurança da informação.

Considera-se, também, neste estudo, que o comportamento informacional (as necessidades, a busca e o uso da informação) dos profissionais que atuam na segurança cibernética da APF, pode variar de acordo com: o ambiente organizacional, a área específica de atuação, a função exercida de cada servidor público, as TICs envolvidas e a criticidade dos sistemas de informação gerenciados. Destaca-se, ainda, que o comportamento informacional pode ser analisado por intermédio do estudo de usuários da informação, uma temática em constante evolução na área da Ciência da Informação. A coerência da escolha encontra respaldo em Casado (1994), ao caracterizar estudo de usuários como:

> o conjunto de estudos que tratam de analisar qualitativa e quantitativamente os hábitos de informação dos usuários mediante a aplicação de distintos métodos, entre eles os matemáticos - principalmente estatísticos - a seu consumo de informação.

Dessa forma, e em face do incremento do uso das TIC pelo governo brasileiro e pela sociedade em geral, do aspecto essencial da ação humana na efetividade das soluções de segurança implementadas, bem como pela indiscutível necessidade em manter os sistemas de informação e as redes de computadores governamentais disponíveis, confiáveis e íntegros, justifica-se analisar, no âmbito da Ciência da Informação, o comportamento informacional dos profissionais que atuam diretamente na segurança cibernética da APF.

Assim sendo, considerando-se um escopo mais abrangente e holístico, espera-se que a presente pesquisa possa, também, contribuir nos seguintes aspectos:

a) do ponto de vista de aplicação prática, acredita-se que este trabalho gerará novas e exequíveis possibilidades para o processo de gerenciamento da segurança no contexto do espaço cibernético da APF;

b) pelo aspecto epistemológico da interdisciplinaridade, almeja-se que, além das contribuições objetivas centradas na segurança em um espaço informacional típico,

como o cibernético, a pesquisa colabore com as discussões sobre segurança da informação, cibernética e comportamento informacional no contexto da Ciência da Informação;

c) no macroambiente político-social do setor cibernético brasileiro, espera-se que os resultados obtidos com a presente pesquisa contribuam para a melhoria dos níveis de segurança da informação e de segurança cibernética nas organizações, independentes de serem públicas ou privadas.

1.5 Organização da Dissertação

O restante dessa dissertação é composto por mais cinco capítulos, referências e dois apêndices.

O Capítulo 2 apresenta uma revisão da literatura e dos conceitos empregados na pesquisa. O Capítulo 3 apresenta e justifica a metodologia empregada na coleta, análise e discussão dos dados. O Capítulo 4 apresenta e analisa os dados e resultados obtidos. O Capítulo 5 discute sobre os resultados à luz da literatura. O capítulo 6 apresenta as conclusões, as limitações e as possibilidades futuras de aprofundamento do trabalho.

São apresentadas 111 referências a fontes de informação bibliográficas consultadas pelo autor durante o estudo. Os Apêndices apresentam o questionário e o roteiro da entrevista empregado pelo autor.

2 REVISÃO DA LITERATURA

Na estruturação da pesquisa foi fundamental considerar o relacionamento entre a Ciência da Informação (CI) e as Tecnologias da Informação e da Comunicação (TIC) que suportam os sistemas de informação, bem como o papel da segurança nesse relacionamento. Em relação ao uso da tecnologia no mundo contemporâneo, Rubin (2010 *apud* Sacerdote, 2013) afirma que as novas tecnologias de informação influenciam quase todos os aspectos de nossas vidas, especificamente alterando a nossa forma de criar, organizar, armazenar e disseminar informações. De forma ratificadora, nas pesquisas realizadas por Zins (2007), foi mapeado que a CI preocupa-se com a criação, disseminação e utilização do conhecimento, possuindo duas subáreas, a saber: uma relacionada aos aspectos humanos e sociais e outra aos aspectos técnicos que são os sistemas de informações.

De acordo com Le Coadic (1996), interdisciplinaridade traduz-se pela colaboração entre diversas disciplinas, que leva a interações, isto é, a certa reciprocidade, de forma que haja enriquecimento mútuo. Assim, por esse aspecto epistemológico interdisciplinar, pode-se deduzir, então, que a CI envolve, também, o estudo da informação e a sua interação com as TIC. Por sua vez, o uso intensivo das TIC como suporte de informação não traz apenas vantagens. No seu bojo, encontram-se, ainda, os problemas e os riscos inerentes ao uso dos sistemas e das redes de dados, principalmente os relativos à segurança das informações disponibilizadas e comunicadas. Neste contexto, Capurro (2003) lembra que a rede digital provocou uma revolução não apenas midiática, mas também epistêmica com relação à sociedade dos meios de comunicação de massa do Século XX. Essa estrutura permite um modelo interativo que vai além das tecnologias de intercâmbio de mensagens, criando novos problemas sociais, econômicos, técnicos, culturais e políticos [de segurança], os quais mal começamos a enfrentar na teoria e na prática.

Apresenta-se, assim, uma revisão da literatura orientada aos objetivos da pesquisa, abordando os principais conceitos teóricos ligados: (1) às características peculiares da cibernética e do espaço cibernético, onde estão inseridos os sistemas de informação; (2) à organização da segurança da informação enquanto atividade prática com significativa normatização, e de sua aplicabilidade no contexto da APF, (3) à segurança cibernética, particularmente no tocante a um agente público que atue na gestão da segurança do espaço cibernético no âmbito da APF; e (4) aos estudos de usuário da informação.

Ao se ressaltarem as ligações da CI com as TIC, bem como com a segurança da informação, percebe-se que o ser humano, independente da quantidade e qualidade de artefatos

de TIC empregados, continua sendo peça fundamental e indispensável em qualquer estrutura ou processos de segurança de sistemas de informação.

A revisão da literatura sobre o Estudo de Usuários da Informação teve a finalidade de discernir quais seriam os métodos e abordagens mais coerentes e alinhados com as tipicidades e características inerentes ao objeto de estudo.

Por conseguinte, foi priorizada a fundamentação teórica nos assuntos quanto às necessidades, fontes e canais de informação, com a finalidade de compreender, mais profundamente, o comportamento informacional dos responsáveis por gerir os incidentes de segurança cibernética da APF.

Especial deferência foi destinada às revisões, pesquisas e estudos realizados por pesquisadores nacionais contemporâneos, na busca por "leituras" e abordagens atualizadas, customizadas com características do contexto brasileiro. Interessante registrar que as visões e entendimentos, por vezes diferenciados, ao invés de esgotar o tema, possibilitam novos horizontes e desafios de pesquisa, enriquecendo a Ciência da Informação.

2.1 A Cibernética e os Sistemas

2.1.1 Sistemas de Informação e o Espaço Informacional

Na essência, o conceito de sistema contempla um grupo de elementos (que formam um todo unificado) inter-relacionado e o todo que organiza as partes. De acordo com Ballestero-Alvarez (1997), Von Bertalanffy, precursor da Teoria Geral dos Sistemas (TGS), ao comparar sistemas nas diversas áreas das Ciências Físicas, concluiu que alguns conceitos básicos de sistemas eram suscetíveis de aplicação em outros campos da ciência, como a cibernética. Não obstante, o sistemismo, também conhecido como enfoque sistêmico: "possui sua originalidade, retirada principalmente da teoria da informação, da cibernética e de sua utilização administrativa" (DEMO, 1995, p. 203).

Norbert Wiener (1968, p.17) [5] sinaliza a importância da informação para a Cibernética, ao sintetizar o conceito de informação como

> o termo que designa o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que nosso ajustamento seja nele percebido. O processo de receber e utilizar a informação é o processo de nosso ajuste às contingências do meio ambiente e de nosso efetivo viver nesse meio ambiente.

[5] Considerado um dos fundadores da Cibernética contemporânea.

No âmbito da Ciência da Informação, ao refletir sobre os diversos aspectos que envolvem a conceituação de informação, Lins (2013) aborda o conceito prático da informação, quando é utilizada a expressão sistemas de informação para designar processos tecnológicos que determinam um fluxo de dados organizados em um suporte para necessidades gerenciais. Ainda no contexto da CI, o Conarq (2011) define sistema de informação (SI) como o conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação.

Na perspectiva organizacional, Ansoff (1990) demonstra como principal característica sistêmica da organização, a sua inter-relação com o ambiente que a cerca e a necessidade de mudança do sistema, para que ele possa continuar a existir, denominada "superação" pela TGS. Fernandes (2009, p.1), salienta que "um sistema de informações é uma rede de relacionamentos interpessoais sistemicamente organizada no ambiente de trabalho através do suporte da TI". O referido autor acrescenta que

> no âmbito da TI, um sistema de informações pode ainda ser definido como um espaço informacional onde se realizam fluxos de informação (processos) de natureza específica, relativos a uma determinada área, função ou nível de atuação da organização, no qual convivem pessoas com o suporte das interfaces e serviços providos pela TI, visando à produção de um conjunto consistente de informações [...].

Em relação a espaço informacional, Cavalcanti e Cunha (2008, p.155) consideram o mesmo como: "o campo que existe em um novo espaço, ligado por redes de informação, caracterizado por: 1) não ter fronteiras, como um campo territorial; 2) os elementos envolvidos em ações orientadas por objetivos orientados através dessa rede".

Na atual conjuntura, os sistemas de informação governamentais estão amplamente suportados pelas TIC, onde as informações situam-se em uma determinada área de interesse que pode, de igual forma, ser denominada espaço informacional.

2.1.2 Espaço Cibernético

O termo cibernética deriva do grego *kybemytiky* e significa arte de governar navios (ou homens), isto é, dirigi-los por meio da comunicação e do controle, ou seja, a arte do piloto. No campo científico e partindo de análises comportamentais, Wiener (1968) apresenta cibernética como o estudo da comunicação e controle das máquinas, seres vivos e grupos sociais; considerando que, do ponto de vista da transmissão da informação, não há distinção entre máquinas e seres humanos. Wiener (1968, p.17), prossegue seus estudos ao esclarecer que

> o propósito da cibernética é o de desenvolver uma linguagem e técnicas que nos capacitem, de fato, a haver-nos como problema de contrôle e da comunicação em geral, e a de descobrir o repertório de técnicas e idéias adequadas para classificar-lhe as manifestações específicas sob a rubrica de certos conceitos.

Para Chiavenato (2003, p. 414-418), a Cibernética é uma ciência relativamente jovem, que teve origem no movimento iniciado por Norbert Wiener para esclarecer as chamadas "áreas brancas no mapa da ciência". A Cibernética começou como uma ciência interdisciplinar de conexão entre as ciências, tendo sido assimilada pela Informática e pela Tecnologia da Informação (TI). O autor aborda Cibernética como:

> a ciência da comunicação e do controle, seja no animal (homem, seres vivos), seja na máquina. A comunicação torna os sistemas integrados e coerentes e o controle regula o seu comportamento. A Cibernética compreende os processos e sistemas de transformação da informação e sua concretização em processos físicos, fisiológicos, psicológicos etc. Na verdade, a Cibernética é uma ciência interdisciplinar que oferece sistemas de organização e de processamento de informações e controles que auxiliam as demais ciências.

Aprofundando o tema, espaço cibernético (tradução de *Cyberspace*) descreve o terreno não físico criado pelos sistemas computacionais e pelas redes de comunicações. Tal termo foi criado por Willian Gibson, em Neuro romancer (1984), para relacionar o mundo e a sociedade que se reúnem ao redor do computador. Para Gibson, o ciberespaço seria uma rede futurística de computadores (atual Internet) que as pessoas usariam, conectando seus cérebros à mesma (CAVALCANTI; CUNHA, 2008).

Elias (2001) sugere Espaço cibernético ou Ciberespaço como "uma metáfora que descreve o terreno não físico criado por sistemas de computador. [...] Como espaço físico, o ciberespaço contém objetos (arquivos, mensagens de correio, gráficos, etc.) e modos diferentes de transporte e entrega de dados". Interessante ressaltar que o chamado espaço cibernético não se encontra restrito ao uso da Internet ou dos computadores, como corrobora Klimburg (2012, tradução nossa): "o ciberespaço é mais do que a Internet, incluindo não somente o *hardware*, *software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes". [6]

Nesta pesquisa, entende-se que o espaço cibernético de uma organização da APF enquadra-se nas características supracitadas, particularmente por serem grandes proprietárias e usuárias de complexos sistemas de informação suportados por estruturas informatizadas e por redes de computadores nacionais ou globais (Internet).

---

[6] *Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks.*

2.2 Segurança da informação

No âmbito da Área do conhecimento da CI, segurança da informação seria assegurar que a produção, seleção, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação estivessem livres de perigos e incertezas (GRIFFITH *apud* CAPURRO, 2003; RAMOS, 2006).

No contexto interdisciplinar[7], inerente à CI e em relação à tríade da segurança da informação (CID), conclui-se que: a confidencialidade se relaciona com níveis de sigilo da informação, a integridade com proteção contra alterações em seu estado original e a disponibilidade com atendimento oportuno de uma demanda informacional. As propriedades da segurança da informação são, assim, definidas com base na ISO/IEC 27000 (2014):

a) confidencialidade (*confidentiality*) - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

b) integridade (*integrity*) - propriedade de exatidão e completeza;

c) disponibilidade (*availability*) - propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada;

d) autenticidade *(authenticity)* - propriedade de que uma entidade é o que a mesma diz ser;

e) responsabilidade *(accountability)* - propriedade na qual o responsável pela informação deve prestar contas da mesma;

f) não repúdio (*non-repudiation*) - capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias;

g) confiabilidade (*reliability*) - propriedade de que o comportamento e o resultado acham-se consistentes com a intenção.

A ABNT NBR ISO/IEC 27002 (ABNT, 2013) descreve, no seu capítulo introdutório, que segurança da informação "é a proteção[8] da informação de vários tipos de ameaças[9] para garantir a continuidade do negócio, minimizar o risco[10] ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio". A Norma recomenda que, como a informação pode existir e ser compartilhada de diversas formas: impressa ou escrita em papel, armazena-

[7] Além de ser um dos aspectos epistemológicos mais relevantes da CI, a interdisciplinaridade é um fundamento da segurança da informação, pois na sua práxis se inter-relaciona com a Comunicação, a Ciência da Computação, as Leis, a Semiótica, a Educação, a Psicologia entre outros.

[8] Entende-se como ação ou conjunto de ações que proporcionam segurança.

[9] Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2013).

[10] Combinação da probabilidade de um evento e de suas consequências (ABNT, 2013).

da eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas, deva sempre ser protegida. E, em seguida, define segurança da informação como a "preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas" (ratificada pela ISO/IEC 27000 - *Overview and vocabulary*).

As atividades de uma instituição ou empresa, sejam elas ligadas diretamente ao seu negócio (atividades fim) ou à sua vida vegetativa (atividades meio), são apoiadas por processos informacionais, os quais, em essência, também orientam e regulam as tarefas de cada indivíduo no ambiente organizacional. Atualmente, os processos e a dinâmica organizacional são estruturados em sistemas de informação informatizados suportados por ativos de informação[11] que, por serem essenciais para a manutenção dos fluxos de trabalho e dos negócios, devem ser protegidos.

O estabelecimento de controles que protejam estes ativos depende da correta identificação de quais eles sejam, bem como, da definição dos responsáveis pelo ativo, dos usuários que o empregam e do valor relativo que o mesmo tem para a organização (BEZERRA, 2011). Nesta linha de pensamento, Vidal e Fernandes (2013) definem segurança da informação como sendo

> a proteção dos ativos de informação de uma organização contra um grande número de ameaças, visando assegurar ou garantir a continuidade das atividades de negócio ou o cumprimento da missão crítica desta organização, minimizando os riscos às suas atividades, maximizando retorno sobre seus investimentos e as oportunidades de sucesso.

Compilando-se, por meio da interdisciplinaridade, para as áreas de: informática, redes de computadores, Biblioteconomia e Arquivologia, Cavalcanti e Cunha (2008) definem segurança da informação como um conjunto de procedimentos para proteção do acervo informacional de uma organização contra o acesso à informação ou ao seu uso por pessoas não autorizadas. De acordo com o Conselho Nacional de Arquivos - Conarq (2011), segurança é um dos requisitos para sistemas informatizados de gestão arquivística de documentos e caracteriza-se pela preservação de diversos atributos, tais como:

a) confiabilidade: credibilidade de um documento arquivístico enquanto afirmação de um fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação;

[11] São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2009b).

b) integridade: estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada;

c) disponibilidade: prontidão de atendimento de um sistema;

d) autenticidade: credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.

Com um enfoque ao mesmo tempo social e sistêmico, pois reconhece o papel do indivíduo na segurança e admite sua relação estrita com os sistemas de informação, Marciano (2006) define segurança da informação como um fenômeno social no qual os indivíduos possuem razoável conhecimento acerca do uso dos sistemas de informação, o que inclui os ônus decorrentes (riscos negativos) e os papéis que os mesmos devem desempenhar. Sintetizando, segurança da informação zela por manter íntegros os processos informacionais que servem à organização em um determinado contexto, seguindo os requisitos gerados pela mesma e também aqueles emanados dos indivíduos usuários dos sistemas de informação.

2.2.1 As Normas Técnicas e a segurança da informação

Os modelos conhecidos de melhoria da gestão e governança da segurança da informação são baseados especialmente em normas de origem inglesa[12] (BS-*British Standards***)**, como as da Série ISO/IEC[13] 27000. Por exemplo, a atual norma ISO/IEC 27001, que trata da definição dos requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), teve seu embrião na BS 7799-1:1995-Tecnologia da Informação - Código de prática para gestão de segurança da informação (BASTOS; CAUBIT, 2009).

A série 27000 aborda o tema segurança da informação e incorpora uma família de normas sobre gestão de segurança da informação, gestão de riscos e, mais recentemente, sobre segurança cibernética. O Quadro 1 elenca as normas mais relevantes, em sua maioria traduzidas para o português pela ABNT[14].

---

[12] O Reino Unido é um grande provedor de regras e padronização, pela sua tradição de precursor em atividades de elaboração de padrões desde a Revolução Industrial (BASTOS; CAUBIT, 2009).

[13] ISO (*The International Organization for Standardization*) organização não governamental, com sede na Suíça, que estabelece padrões internacionais para certificação de diversas áreas. IEC (*The International Eletrotechnical Comission*) organização internacional de padronização de tecnologias elétricas e eletrônicas.

[14] Associação Brasileira de Normas Técnicas é o fórum nacional de normalização.

Quadro 1 - A família ISO/IEC 27000

NORMA	NOME	DESCRIÇÃO/OBJETIVO
27000: 2014	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	provides the overview of information security management systems (ISMS), and terms and definitions commonly used in the ISMS family of standards. It is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).
27001: 2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos	especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
27002: 2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação	fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
27003: 2011	Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um SGSI	foca os aspectos críticos necessários para a implantação e projeto bem sucedidos de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com a ABNT NBR ISO IEC 27001:2005.
27004: 2009	Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição	fornece diretrizes para o desenvolvimento e uso de métricas e medições, a fim de avaliar a eficácia de um Sistema de Gestão de Segurança da Informação (SGSI) implementado e dos controles ou grupos de controles, conforme especificado na ABNT NBR ISO/IEC 27001.
27005: 2011	Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação	fornece diretrizes para o processo de gestão de riscos de segurança da informação.
27007: 2012	Diretrizes para auditoria de sistemas de gestão da segurança da informação	fornece diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI) e sobre como executar as auditorias e a competência de auditores de SGSI, em complementação às diretrizes descritas na ABNT NBR ISO 19011.
27008: 2011	Information technology -- Security techniques -- Guidelines for auditors on information security controls	This standard (actually a “technical report”) on “technical auditing” complements ISO/IEC 27007. It concentrates on auditing the information security controls, whereas ’27007 concentrates on auditing the management system elements of the ISMS (SGSI).
27014: 2013	Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação	fornece orientação sobre conceitos e princípios para a governança de segurança da informação, pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a segurança da informação dentro da organização.
27032: 2012	Information technology -- Security techniques -- Guidelines for cybersecurity	provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP).
27037: 2013	Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital	fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

Fonte: adaptado da ABNT (catálogo)[15]

[15] Disponível em: <http://www.abntcatalogo.com.br>. Acesso em: 30 mar. 2014.

As normas 27001 e 27002 formam a base da família 27000, fornecendo uma visão estruturada da gestão da segurança da informação. Para tanto, adotam um paradigma sistêmico, baseado na seleção e implementação gradual de controles de segurança, por meio do ciclo da melhoria da qualidade: o ciclo PDCA (*Plan, Do, Check, Act*). De acordo Bastos e Caubit (2009), as respectivas normas propõem a

> integração dos dispositivos de proteção de maneira organizada, contemplando um ciclo de revisões periódicas e melhoria contínua, dimensionadas de acordo com as necessidades de segurança da informação estabelecidas para o negócio [público ou privado] da organização.

As normas 27001 e 27002 são organizadas em seções (que vêm se ampliando a cada revisão), onde são apresentados objetivos, controles e diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI). As instituições, que se adaptam aos requisitos e às boas práticas do SGSI proposto, reúnem condições de serem certificadas em um padrão internacional.

A recente norma 27032, que trata da segurança cibernética, traça um panorama geral da segurança no espaço cibernético: os "envolvidos", ativos, controles, vulnerabilidades[16] e ameaças entre outros aspectos. Aprofundando, mais tecnicamente, o tema segurança cibernética, a Norma 27037 fornece subsídios para o processo investigatório após a ocorrência de um incidente.

2.2.2 Segurança da informação na APF

A atividade de segurança da informação é complexa e heterogênea, particularmente no ambiente governamental, onde foi, inicialmente, regulada pelo Decreto Presidencial n. 3.505, de 13 de junho de 2000 (BRASIL, 2000), que instituiu a política de segurança da informação (PSI) nos órgãos e entidades da APF. Em consequência, desde aquela época, grupos de trabalho, estabelecidos pelo Comitê Gestor de Segurança da Informação (CGSIPR), vêm estudando as diretrizes apontadas no referido decreto e buscando soluções para sua efetiva implementação. Naquela ocasião, a segurança da informação foi definida 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).

[16] Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (ABNT, 2013).

A aplicação do citado decreto mostrou-se de grande complexidade, sendo necessária a publicação de novas normas para discipliná-lo.

A Instrução Normativa n. 1, do Gabinete de Segurança Institucional da Presidência da República (IN 01/GSIPR), de 13 de junho de 2008 (BRASIL, 2008a), disciplinou a Gestão de Segurança da Informação e Comunicações (SIC)[17] na Administração Pública Federal, direta e indireta, determinando, entre outros assuntos, no seu Art. 5º, que aos órgãos e entidades da APF compete: coordenar as ações de segurança da informação e comunicações, aprovar Política de Segurança da Informação e Comunicações e implementar equipe de tratamento e resposta a incidentes em redes computacionais (ETIR)[18].

A IN 01/GSIPR (BRASIL, 2008a) assim entendeu Segurança da Informação e Comunicações: "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações". Dessa forma, a IN01 ampliou a tradicional tríade CID para DICA, onde entende-se que:

a) disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
b) integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
c) confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
d) autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Neste contexto, a IN 01/GSIPR definiu no âmbito da APF a gestão de SIC como

> ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio**,** tratamento de incidentes, tratamento da informação, conformidade, credenciamento, **segurança cibernética** [grifo nosso], segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

A não limitação às TIC fica evidente quando se verifica o amplo escopo da definição e percebe-se que quatro dimensões sintetizam a gestão de SIC: pessoas, tecnologia, processos e ambiente.

---

[17] Na opinião do autor, a adição do termo comunicações, na prática, em nada se desalinha da Segurança da Informação praticada no âmbito da CI.

[18] Conhecido também como *Computer Security Incident Response Team* – CSIRTs (Times de Resposta a Incidentes de Segurança em Computadores) ou CERT - *Computer Emergency Response Team* (Times de Resposta a Emergência em Computadores).

Assim como a "Família 27000", a IN 01/GSIPR gerou um arcabouço de normas complementares (NC) que evidenciam a diversidade de áreas de atuação da gestão de SIC sintetizadas no Quadro 2.

Quadro 2 - Normas complementares à IN 01/GSIPR

NC	DESCRIÇÃO/OBJETIVO
01/IN01 2008	Atividade de Normatização.
02/IN01 2008	Metodologia de Gestão de Segurança da Informação e Comunicações.
03/IN01 2009	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações.
04/IN01 2013	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC. (Revisão 01)
05/IN01 2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR.
06/IN01 2009	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações.
07/IN01 2010	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações.
08/IN01 2010	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais.
09/IN01 2013	Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações. (Revisão 01)
10/IN01 2012	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC.
11/IN01 2012	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações.
12/IN01 2012	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC.
13/IN01 2012	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações.
14/IN01 2012	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC.
15/IN01 2012	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais.
16/IN01 2012	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de *Software* Seguro.
17/IN01 2013	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações.
18/IN01 2013	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações.
19/IN01 2014	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF.
20/IN01 2014	Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação.

21/IN01 2014	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Fonte: adaptado da Legislação - SIC[19]

Como pode, pois, ser percebido, desde o Decreto 3.505 de 2000 até o presente, diversas ações e normatizações foram realizadas, a fim de subsidiar, com critérios uniformes, uma gestão consistente da segurança da informação na APF.

Um retrato recente da situação da SIC na APF está presente nos levantamentos de governança de Tecnologia da Informação efetuados pelo Tribunal de Contas da União - TCU (BRASIL, 2012, 2014b). De maneira particular, a área de segurança da informação continua a chamar a atenção pelos altos índices de não conformidade[20], sugerindo que, de forma geral, as organizações públicas, além de não tratarem dos riscos aos quais estão expostas, desconhecem tais problemas. Percebeu-se que a APF não somente permanece exposta a riscos diversos e não mapeados, como também não está agindo para saneá-los com a agilidade que o caso requer, pois nenhum dos indicadores relativos à segurança da informação, que envolve confidencialidade, integridade e disponibilidade da informação, tem apresentado avanço substancial. A despeito das recomendações emitidas pelo TCU e das publicações normativas sobre esse tema, a APF, de forma geral, continua a desconhecer e a não proteger as próprias informações críticas adequadamente. Infere-se, daí, também, sua reduzida capacidade de gerir incidentes de segurança de média e grande complexidade (WALLIER VIANNA, 2011).

De forma complementar, a coordenação do CEGSIC 2012/2014 (2013), ao justificar a realização do referido curso, clarifica a situação contemporânea da segurança da informação na APF, quando observa, dentre outros aspectos, que:

a) organizações de todos os portes, públicas e privadas, implantam e operam diariamente novos sistemas de informação, sistemas de comunicação e sistemas de controle, cada vez mais críticos às suas próprias atividades;

b) nos órgãos e entidades do poder público, esse ritmo de implantação e operação de sistemas cria cenários de riscos crescentes para o Estado, governos e para a própria sociedade;

c) em contraponto a um pequeno volume de investimentos em pesquisa e inovação de processos de gestão de segurança da informação, há um alto volume de investi-

[19] Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: 30 mar. 2014.

[20] Cumprimento das legislações, normas e procedimentos.

mentos em aquisições no desenvolvimento de sistemas de informação e comunicação;

e) na APF, há deficiência nos quadros de pessoal, quanto à gestão da segurança da informação.

2.3 Segurança Cibernética

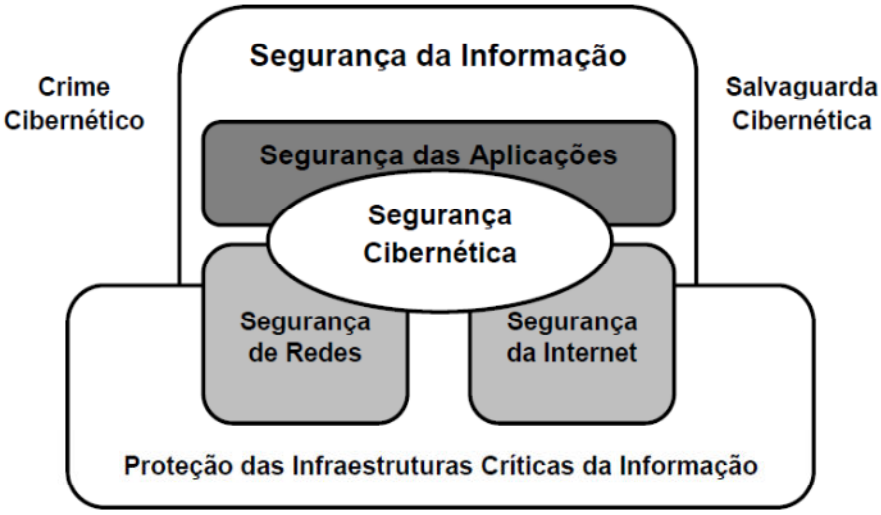
A princípio, poder-se-ia supor que segurança cibernética, também conhecida como segurança digital ou do espaço cibernético, seria uma evolução da segurança da informação. Para o autor desta pesquisa, segurança cibernética encontra-se inserida no contexto mais amplo e multifacetado da segurança da informação, em consonância com o descrito pela Academia Latino-Americana da Segurança da Informação (2006)**:** "a segurança da informação tem como propósito proteger as informações registradas, sem importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem".

No entendimento de Fernandes (2012b), a segurança pode ser obtida por meio da associação de uma hierarquia de controles a um sistema. Para o autor, um sistema seguro é modelado por subsistemas hierarquicamente organizados, cada qual com controles que monitoram e regulam não só a função mais exterior do sistema, mas também todo o complexo arranjo interno do mesmo.

A norma ISO/IEC 27032- *Guidelines for cybersecurity (*Diretrizes para a segurança cibernética*)*, alinhada com o "espírito" de segurança da informação inerente à família 2700, define segurança cibernética (*Cybersecurty* ou *Cyberspace security*) como preservação da confidencialidade, da integridade e da disponibilidade da informação **no espaço cibernético.** Adicionalmente, outras propriedades, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas nesse contexto (ISO/IEC 27032, 2012, tradução e grifo nossos).

A Figura 1, extraída da norma ISO/IEC 27032, exemplifica uma forma de inserção da segurança cibernética no campo da segurança da informação.

Figura 1 - Relacionamento entre segurança cibernética e outras seguranças



Fonte: adaptado de ISO/IEC 27032 (2012)

Percebe-se que a segurança cibernética, além de achar-se inserida no bojo da segurança da informação e da proteção das infraestruturas críticas[21] de informação, permeia a segurança das redes, da Internet e das aplicações (sistemas).

2.3.1 Vulnerabilidades e ameaças cibernéticas

Empresas e instituições como a CISCO (2014), que atuam na segurança das TIC, em escala global, alertam que, em 2013, as vulnerabilidades e ameaças a nível global atingiram os seus mais altos padrões desde 2000.

O cenário internacional tem exposto ações de vigilância e espionagem no mundo digital, comprometendo a soberania dos Estados e erodindo a privacidade de pessoas e de organizações. Tal fato foi evidenciado, em 2013, com a revelação de que o governo dos Estados Unidos realiza espionagem de dados em escala global.

O "caso Snowden" (nome do delator do esquema de monitoramento - Edward Snowden) revelou o *modus operandi* do esquema de espionagem, onde, entre outros fatos, o governo americano possui acesso aos correios eletrônicos (*e-mails*), fotos e ligações dos usuários de serviços de empresas como Google, Microsoft e Facebook, bem como a existência de um programa de vigilância secreta que envolve setores de inteligência de gigantes da Internet. A mídia brasileira publicou diversas matérias sobre o monitoramento de chamadas telefônicas e

[21] São Infraestruturas Críticas às instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2009b).

e-mails brasileiros, inclusive levantando denúncias de espionagem sobre empresas brasileiras como a Petrobrás e a presidência da República. Em âmbito nacional, as repercussões das revelações de Edward Snowden levaram o Senado Federal brasileiro a instaurar uma Comissão Parlamentar de Inquérito (CPI) da Espionagem (SENADO FEDERAL, 2014).

Neste contexto, os ataques simples ou individuais, que causavam males controláveis e prejuízos limitados, deram lugar a operações sofisticadas e bem financiadas do crime cibernético organizado, capazes de causar danos econômicos e de reputação significativos a vítimas dos setores público e privado, atingindo nações e grandes empresas mundiais.

De forma alarmente, ressalta-se a carência de profissionais qualificados em segurança cibernética e a importância deles no monitoramento e na resposta aos incidentes, destacando também, a necessidade de serem encontradas formas de anular estas ameaças, que, cada vez mais, reduzem a confiança dos usuários na segurança *online* dos sistemas, das aplicações e das redes.

Neste ambiente adverso, serão elencadas as principais **vulnerabilidades** que os governos e órgãos públicos podem apresentar:

a) a reduzida preocupação da alta administração com o uso e a gestão da TI institucional, o que pode induzir à ineficiência e à falta de efetividade da instituição como um todo;

b) a maioria das organizações públicas não têm os cuidados necessários com a segurança da informação, na sua expressão mais abrangente (incluindo pessoas, processos e tecnologia), o que coloca, em grande risco, não somente as próprias organizações, mas também o cidadão brasileiro cujos dados estão sob a custódia da Administração Pública;

c) a limitada proteção dos ativos de informação contra ataques cibernéticos, incluídos no rol dos mesmos: motivações políticas e sociais que podem conduzir ao desfiguramento de *sites* (sítios *Web*) com inserções de propaganda adversa e apropriações indevidas de informações em bases de dados de acesso restrito;

d) a carência de legislação específica, atual e com penas severas, o que amplia a sensação de impunidade, podendo ser fator indutor de instalação de bases cibernéticas para terroristas, fraudadores bancários, narcotraficantes e criminosos em geral (WALLIER VIANNA, 2013b).

A Internet[22] tornou-se importante ferramenta tecnológica para grupos dos mais diversificados interesses, extremistas ou não, tendo em vista que o mundo virtual propicia um ambiente seguro para os mesmos. Por conseguinte, destacam-se as **ameaças** mais factíveis de acontecer no atual cenário cibernético internacional e em relação à APF:

a) uma ação cibernética hostil (também denominada de ataque cibernético) por grupos antagônicos às infraestruturas críticas, que pode ser empregado como multiplicador de efeitos, ao potencializar os danos causados por um ataque físico (causador de pânico imediato com imagens de fogo e destruição, por exemplo), mediante obstaculização ou desinformação;

b) divulgação de boatos, realização de sabotagem ou mesmo espionagem comercial e industrial cibernéticas, em relação às infraestruturas críticas brasileiras ou mesmo em segmentos econômicos privados, por atos de grupos internacionais interessados em comprometer a imagem, o funcionamento ou o desenvolvimento dos mesmos;

c) sabotagem ou protestos durante a preparação e a realização dos grandes eventos internacionais, por grupos estrangeiros ou mesmo ativistas nacionais, com interesses em macular a imagem do Brasil no contexto internacional (WALLIER VIANNA, 2013b).

2.3.2 Incidentes de segurança cibernética

O profissional de segurança cibernética, invariavelmente, pode deparar-se com o planejamento, a implantação e a manutenção de infraestruturas de TIC. É importante salientar que qualquer infraestrutura de TIC pode ser alvo de ataques cibernéticos, e os danos causados à mesma recaem, genericamente, sobre três categorias elementares:

a) indisponibilidade - nesse caso, os sistemas passam a não responder dentro de prazos oportunos e previstos;

b) adulteração de informações - as respostas deixam de ser confiáveis, por terem sido alteradas;

c) acesso não autorizado - os sistemas permitem que terceiros (pessoas ou computadores) não autorizados acessem informações privilegiadas, ou obtenham o próprio controle operacional do sistema.

[22] O termo por vezes é usado como um sinônimo para espaço cibernético (CAMPELO; CALDEIRA, 2005).

Por sua vez, um ataque cibernético pode ocorrer sob diversas formas, sendo as mais relevantes:

a) instalação de um programa ilícito como vírus, cavalos de troia ou *spywares*[23];

b) negação de serviço disponibilizado (*Denial-of-Service* (DoS));

c) introdução de funcionalidades não autorizadas nos sistemas operacionais (de forma que estes passem a reconhecer o acesso do atacante, privilegiando-o com permissões especiais, ao garantir que seu trânsito no sistema seja absolutamente livre, inclusive não rastreável pelas rotinas de auditoria) de amplo emprego, como microcomputadores e servidores padronizados de uso genérico;

d) inserção de vulnerabilidades em sistemas estratégicos, como a referente a comandos não documentados que tornariam possível a terceiros (mais exatamente, a seus próprios programadores) desabilitar ou alterar a operacionalidade desse sistema crítico;

e) *hacking:* exploração das vulnerabilidades que inevitavelmente se manifestam em qualquer arcabouço de controles e sistemas integrados numa rede;

f) infiltração de pessoas (*insiders*) com objetivos diversos, tais como: disponibilização de senhas que permitam o acesso externo de terceiros não autorizados e instalação prévia de programas hostis que produzam ou facilitem o ataque e modificações de *hardware* (WALLIER VIANNA, 2013b).

Em relação aos eventos que comprometam a segurança das informações, a Norma Complementar n. 05/IN01/DSIC/GSIPR (BRASIL, 2009a) define que um incidente de segurança "é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores". No trato de incidentes de segurança, podem ser observados:

a) tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados;

b) interrupção indesejada ou negação de serviço;

c) uso não autorizado de um sistema para processamento ou armazenamento de dados;

d) furto de informação sigilosa em formato digital;

e) extorsão via o uso de computadores;

---

[23] Vírus: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo copias de si mesmo, tornando-se parte de outros programas e arquivos; cavalos de troia: programa normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário; *spywares:* programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. (CERT.br, 2012)

f) modificações nas características de *hardware, firmware* ou *software* de um sistema, sem o conhecimento, instruções ou consentimento prévio do responsável pelo sistema;

g) obtenção, guarda e preservação de evidências;

h) detecção (monitoração de redes e sistemas para detecção da intrusão, ou da suposta tentativa);

i) violação ou quebra da Política de Segurança de forma explícita ou implícita.

A gestão e a consequente resposta a incidentes, segundo o modelo desenvolvido pelo *Computer Emergency Response Team* vinculado a Carnegie Mellon University - CERT-CC, envolve diversas atividades que são enquadradas em três tipos de serviços: reativos, proativos e gestão de qualidade de segurança, descritos a seguir:

a) Serviços Reativos:

- realizar alertas;
- tratar incidentes (detecção, triagem, análise, resposta);
- tratar vulnerabilidades;
- tratar artefatos.

b) Serviços Proativos:

- notificações;
- vistorias técnicas;
- avaliação de segurança e auditorias;
- suporte e configuração de ferramentas de segurança, aplicações e infraestrutura;
- desenvolvimento de ferramentas de apoio à segurança;
- serviços de detecção de intrusos;
- disseminação de informações relacionadas à segurança.

c) Serviços de Gestão de Qualidade da Segurança:

- análise de risco;
- planejamento de continuidade do negócio e recuperação de desastres;
- consultoria de segurança;
- construção de consciência da importância da segurança;
- educação/treinamento;
- certificação ou avaliação de produtos (WALLIER VIANNA, 2013b).

2.3.3 Profissionais de segurança cibernética

Para fins deste estudo, considera-se que as atividades inerentes à segurança cibernética estão inseridas no contexto mais abrangente da segurança da informação. Ou seja, o profissional, que atua na segurança cibernética, também "realiza" segurança da informação. A segurança cibernética, além de herdar diversas características da segurança da informação, carrega, no seu bojo, a necessidade de resposta rápida, particularmente em face dos eventos de segurança[24] que venham a ocorrer.

No caso do grupo de usuários, objeto da presente pesquisa, o senso de utilidade imediata da informação é fator determinante diante da necessidade premente por soluções rápidas e pontuais. Essa tempestividade é típica dos problemas cotidianos de segurança cibernética, particularmente no tratamento e resposta a incidentes de redes computacionais. O caráter de urgência é inerente ao grau de comprometimento e importância dos sistemas envolvidos e não deve ser confundido com a quantidade ou com a frequência dos eventos de segurança. Não obstante, o profissional que atua na segurança cibernética deve procurar ser proativo, auditando frequentemente os sistemas e serviços disponibilizados, em busca de vulnerabilidades (que devem ser corrigidas) e levantar as possíveis ameaças (que podem ser mitigadas).

Cabe destacar que, no caso de um evento de segurança configurar-se em um incidente, os prejuízos são mais abrangentes do que em uma organização privada. Tal fato se explica por comprometer-se a manutenção da soberania do Estado brasileiro e das ações governamentais, trazendo significativos prejuízos à cidadania e à sociedade, além das eventuais perdas financeiras; da alocação de recursos humanos e financeiros para a solução dos problemas; do comprometimento da imagem, bem como do negócio da instituição. Neste sentido, tal questão incrementa, exponencialmente, o senso de responsabilidade do agente público alocado na gestão dos incidentes.

Outro fator a ser considerado são os contextos complexos e dinâmicos (de TIC), onde os eventos de segurança ocorrem, gerando por vezes situações-problema inéditas no ambiente organizacional. Sem dúvida, esses fatores típicos e rotineiros do ambiente de trabalho dos profissionais em tela, bem como a necessidade de forte interação com outros indivíduos envolvidos no processo de gerenciamento de incidentes, são elementos geradores de elevado estresse laboral, influenciando diretamente o comportamento informacional e envolvendo, da mesma forma, as dimensões emocional, cognitiva e situacional. Via de regra, observa-se uma

[24] Considera-se como evento de segurança qualquer indício, fato, relato, comprovado ou não, que possa ser relacionado à segurança do espaço cibernético.

limitação de respostas passíveis de serem adotadas, nos casos comprovados de incidentes de segurança. Dos seis tipos de respostas para anomalias ou indicadores dos problemas descritos por Westrum (2004, p. ii25 *apud* Macintosh-Murray e Choo, 2006), apenas duas, no entendimento deste pesquisador, são, na prática, possíveis de utilização no âmbito da segurança do espaço cibernético governamental:

a) Supressão - prejudicando ou parando a pessoa que traz a anomalia à luz;

b) Encapsulação - isolando o mensageiro, com o resultado de que a mensagem não está audível;

c) Relações públicas – apresentando a mensagem "em contexto" para minimizar seu impacto;

d) Reparo local (*Local fix*) - respondendo ao caso atual, mas ignorando a possibilidade de um outro em diferente parte;

e) Reparo global (*Global fix*) - uma tentativa de responder ao problema onde quer que ele exista, como é comum na aviação, quando um único problema dirigirá a atenção aos similares em outra parte;

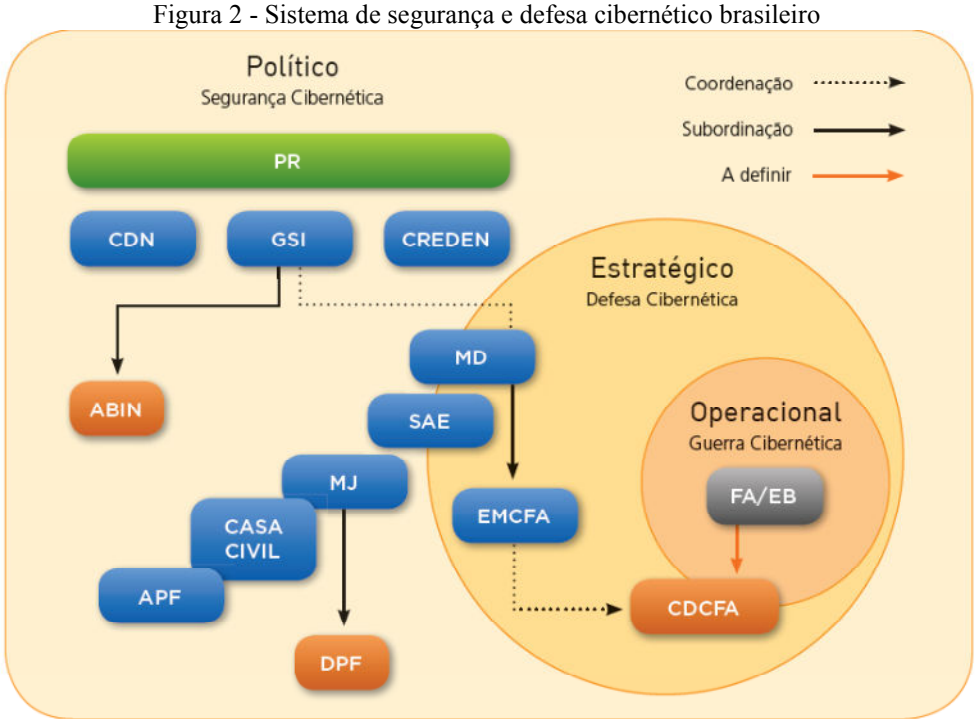
f) Inquérito - Tentar chegar à "causa original" do problema.

2.3.4 Segurança, Defesa e Guerra cibernéticas

Para o Ministério da Defesa, o espaço virtual ou cibernético é composto de dispositivos computacionais conectados em redes, ou não, onde as informações digitais transitam e são processadas e/ou armazenadas (BRASIL, 2011). No que concerne à APF, o conceito de segurança cibernética ainda está em fase de construção e consolidação. No entendimento do Grupo Técnico de Segurança Cibernética, instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), segurança cibernética é a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas (BRASIL, 2009b).

Em dezembro de 2010, a Secretaria de Assuntos Estratégicos da Presidência da República (SAE) promoveu uma Reunião Técnica sobre Segurança e Defesa Cibernética, buscando "identificar o papel desenvolvido pelas Forças Armadas e de outras instituições do Estado brasileiro na área, bem como de outros órgãos públicos e privados envolvidos ou relacionados" (FREITAS; GOMES; RÊGO BARROS, 2011). Outro objetivo foi uma proposta sistêmica para a segurança e defesa cibernética nacional, conforme representada na Figura 2.

Figura 2 - Sistema de segurança e defesa cibernético brasileiro



Fonte: Freitas; Gomes e Rêgo Barros (2011)

O diagrama envolve diversos órgãos públicos enlaçados com o setor cibernético, nos níveis político, estratégico e operacional. Percebe-se que, no bojo da segurança cibernética, faz-se necessário desdobrar dois conceitos relevantes: defesa cibernética e guerra cibernética. De acordo com o Glossário das Forças Armadas (BRASIL, 2007):

> **Defesa Cibernética** é o conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente;
>
> **Guerra cibernética** é o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário, baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil.

No campo da Defesa Nacional, ambiente cibernético refere-se ao uso de redes de computadores e de comunicações e sua interação dentro dos sistemas utilizados por instituições públicas e privadas, de cunho estratégico, incluindo os recursos informatizados que compõem o Sistema Militar de Comando e Controle, bem como os sistemas de armas e vigilância (BRASIL, 2007). A fim de exemplificar, de forma prática e realística, as definições e conceitos supracitados, bem como as graves consequências que ações hostis podem infligir contra o ambiente cibernético de um País, tomar-se-ão, a título de estudo de caso, dois acontecimentos recentes internacionais: os ataques cibernéticos em grande escala sofridos pela Estônia em 2007 e a Guerra da Geórgia em 2008. Em 2007, a Estônia viria a ser alvo do pri-

meiro ataque virtual da história perpetrado contra um Estado-Nação. Extremamente dependente de redes de computadores em serviços públicos e privados, teve suas principais infraestruturas paralisadas por cerca de duas semanas[25], em virtude de um ataque massivo de negação de serviço (*Distributed Denial of Service* - DDoS).

Na opinião de Ashmore (*apud* Rustici, 2012):

> a comunidade de *hackers* russos paralisou os meios de comunicação, algumas operações bancárias e *sites* do governo durante alguns dias, em retaliação à decisão do governo estoniano de retirar de Tallinn um monumento às Forças Armadas soviéticas. Entretanto, como não houve uma intervenção militar correspondente para tirar proveito dos efeitos da campanha cibernética, o impacto foi, de modo geral, financeiro e de curto prazo.

Consequência imediata, ainda em 2008, foi a criação do NATO *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), Centro de Cooperação de Defesa Cibernética da Organização do Tratado do Atlântico Norte (OTAN) com sede em Tallin, naquele mesmo país.

No caso da Geórgia, os ataques cibernéticos foram coordenados com uma operação militar russa, servindo como multiplicadores do poder de combate (RUSTICI, 2012). De fato, a ocupação de parte da Geórgia por forças russas foi antecedida por ataques cibernéticos desencadeados com objetivos bem definidos, como o de calar a mídia georgina, diminuindo a repercussão da ocupação e possíveis retaliações do Ocidente. Outro aspecto interessante, deve-se ao fato de que a guerra cibernética, também, foi empregada para maximizar um alvo puramente econômico:

> quando a Rússia invadiu a Geórgia, grande parte de suas operações militares concentrou-se em tomar não as áreas habitadas por russos étnicos, e sim os portos e instalações georgianos do setor de petróleo e gás. As instáveis condições no terreno, intensificadas por ataques cibernéticos, logo fizeram com que todos os oleodutos georgianos não parecessem confiáveis (OLSON, 2012).

Shakarian (2011) especula que as operações cibernéticas russas podem ter sido originadas por três maneiras: "por 'hacktivistas[26]' patrióticos que reagiram aos ataques contra sítios Internet da Ossétia do Sul; unicamente pelo crime organizado russo e pelo crime organizado russo, a pedido do Kremlin". Ainda segundo Shakarian, foram identificadas duas fases na campanha cibernética russa:

---

[25] A Estônia está classificada entre os países mais conectados e tecnologicamente avançados do mundo, com altos níveis de alfabetização em informática e conectividade, possuindo quase todos os seus serviços públicos e atividades cotidianas integrados em sistemas informatizados e na Internet (mais de dois terços da população têm acesso regular). O *status* da nação báltica como um "e-país" avançado deve-se à iniciativa do governo de incluir a Estônia na economia global, após reaver sua independência no início da década de 1990. Maiores informações disponíveis em **Estônia Torna-se E-stônia (**Ejournal USA, 2010**).**

[26] Hacktivismo (palavra criada pela junção de *hack (er)* e ativismo) pode ser definido como o uso das TICs (particularmente da Internet) para fins políticos e sociais, como forma de promover a expressão política, a liberdade de expressão, os direitos humanos, ou a informação ética.

a) na primeira, *hackers* iniciaram um ataque distribuído de negação de serviço contra sítios Internet do governo da Geórgia e da mídia local, apenas um dia antes do desencadeamento da campanha terrestre. Tal fato levou muitos especialistas a sugerirem que os *hackers* sabiam a data da invasão;

b) na segunda fase, os sítios Internet da mídia e do governo georgianos continuaram a receber os ataques, mas a operação cibernética russa foi ampliada, incluindo instituições financeiras, empresas, instituições de ensino, mídia ocidental (BBC e CNN) e um sítio internet de *hackers* da Geórgia.

Os ataques contra esses servidores não apenas incluíram negação de serviço, mas também a desfiguração de sítios (um exemplo foi a "grafitagem" pró-Rússia nas páginas do governo) e uma campanha de proliferação de mensagens eletrônicas (*spam*) contra políticos georgianos.

Tanto no caso da Estônia quanto na guerra da Geórgia, verifica-se que importantes infraestruturas estratégicas foram abaladas (falhas na segurança e na defesa cibernéticas), comprometendo a soberania e a estabilidade econômica dos países envolvidos. Sem o reconhecimento formal por parte do governo opositor ou a prova indiscutível da responsabilidade dos ataques, os países hostilizados não puderam "declarar" guerra cibernética.

2.4 Estudos de usuários da informação

O campo de Estudo de Usuários (EU) pode ser caracterizado como uma das subáreas da Ciência da Informação e consiste na pesquisa para saber o que as pessoas necessitam em termos de informação ou se as mesmas estão satisfeitas e sendo atendidas adequadamente pelos seus provedores. Neste contexto, considera-se que "usar a informação é trabalhar com a matéria informação para obter um efeito que satisfaça a uma necessidade informacional" (LE COADIC, 1996, p. 39). Esses estudos compreendem, também, a investigação de como e para quê a informação é utilizada pelos usuários[27], assim como essas necessidades são expressas e conhecidas dentro de uma área temática (FIGUEIREDO, 1994; CAVALCANTI; CUNHA, 2008).

Figueiredo (1994) revisa três conceitos basilares para o entendimento de EU:

a) necessidade é o que o indivíduo deve ter para o seu trabalho, pesquisa, edificação, recreação etc., sendo uma demanda em potencial;

[27] Pode-se definir usuário como uma pessoa que se relaciona com a informação, através dos diversos canais de acesso a essa informação (CAVALCANTI; CUNHA, 2008).

b) demanda é o que o indivíduo pede, o item de informação requisitado, sendo um uso em potencial;

c) o uso é aquilo que o indivíduo realmente utiliza, podendo ser indicador de uma demanda e representar uma necessidade de algum tipo.

Para a autora, tais conceitos dependem dos valores da sociedade, da expectativa de satisfação, da disponibilidade e acessibilidade; sendo, portanto, difícil estabelecer relações entre as necessidades, as demandas e os usos da informação. A maioria dos estudos, neste campo, foi realizada a partir da segunda metade da década de 40, com destaque para a Conferência da Royal Society, em 1948, e a Conferência Internacional de Informação Científica, que contribuíram para o desenvolvimento de pesquisas orientadas à temática de estudos de usuários. A partir dessas conferências:

> foi sendo criada uma massa de estudos sobre padrões de coleta de informações, sobre o fluxo da informação nas organizações e sobre as necessidades e demandas de informação de cientistas, tecnólogos, psicólogos, sociólogos, economistas, administradores da área governamental e outros (*op. cit.*).

Não obstante, Cendón e Rolim (2013) esclarecem que alguns autores apontam, também, como marco inicial para os 'estudos de usuários da informação', os estudos de 1930 da Escola de Chicago, desenvolvidos para a integração de grupos imigrantes na comunidade americana, através da biblioteca pública.

Figueiredo (1994) esclarece que: "os estudos orientados aos usuários propriamente ditos não são limitados a uma instituição, mas investigam o comportamento de uma comunidade inteira na obtenção da informação [...]" e que, através dos anos, centenas de estudos foram realizados, possibilitando destacar algumas tendências ou generalizações:

a) acessibilidade e facilidade do uso são os fatores mais determinantes para a utilização ou não de um serviço de informação; o canal mais acessível, embora não o melhor, é escolhido primeiro e, assim, considerações sobre qualidade e confiabilidade são secundárias;

b) muitos profissionais sentem existir um volume excessivo de informação, necessitando de seletividade por parte dos sistemas de informação;

c) há necessidade de que a informação seja corrente, assim a disseminação da informação deve ser mais rápida e eficiente;

d) os canais informais de comunicação são considerados mais importantes do que os canais formais, para satisfazer muitos tipos de necessidades de informação.

Baptista e Cunha (2007) exemplificam, por intermédio de duas importantes fontes de consulta: o *Annual Review of information Science and Tecnology* (ARIST) [28] e o *Library and Information Science Abstracts* (LISA) [29], o crescimento, ao nível mundial, da literatura sobre estudo de usuários. No caso do LISA, a temática referente ao estudo de usuários é uma das mais volumosas em termos mundiais e vem crescendo de produção a cada década. Em relação ao ARIST, a evolução do estudo de usuários pode ser acompanhada pelo Quadro 3.

Quadro 3 - Artigos do ARIST relacionados ao tema Estudo de Usuários

ANO	VOL.	AUTOR (ES)	TÍTULO/ASSUNTO
1966	01	MENZEL, H.	Usos e nescessidades de informação na Ciência e Tecnologia
1967	02	HERNER, S.; HERNER, M.	Usos e nescessidades de informação na Ciência e Tecnologia (revisão)
1968	03	PAISLEY, W.J.	Usos e nescessidades de informação
1969	04	ALLEN, T. J.	Usos e nescessidades de informação
1970	05	LIPETZ, B. A.	Usos e nescessidades de informação
1971	06	CRANE, D.	Usos e nescessidades de informação
1972	07	LIN, N.; GARVEY, W. D.	Usos e nescessidades de informação
1974	09	MARTYN, J.	Usos e nescessidades de informação
1978	13	CRAWFORD, S.	Usos e nescessidades de informação
1986	21	DERVIN, B.; NILAN, M.	Usos e nescessidades de informação (centrado no usuário)
1990	25	HEWINS, E.T.	Estudos usos e nescessidades de informação (centrado no usuário)
1993	28	METOYER, D.	Estudos usos e nescessidades de informação (*Gatekeepers*)
1996	31	DILON, A; MORRIS, M. G.	Estudos usos e nescessidades de informação (TI)
1999	34	WANG, P.	Estudos usos e nescessidades de informação (centrado no usuário)
2001	35	PETTIGREW, K. E.,FIDEI, R.,BRUCE H.	Comportamento Informacional
2006	40	cap. 7 - CASE, D.	Comportamento Informacional
2006	40	cap. 8 - FOSTER J.	Comportamento Informacional
2006	40	cap. 9 - MACINTOSH, A; CHOO, C	Comportamento Informacional
2007	41	COURTRIGHT, C.	Comportamento Informacional
2008	42	WILSON, T. D.	Comportamento Informacional
2009	43	FISHER, E. K.; JULIEN, H.	Comportamento Informacional
2010	44	cap. 7 - BROWN C.	Comportamento Informacional
2010	44	cap. 12 - DAVENPORT, E.	Comportamento Informacional
2011	45	cap. 1 - WHITTAKER S.	Gerenciamento da informação pessoal

Fonte: ampliado de Batista e Cunha (2007) e de Gasque e Costa (2010)

[28] Maiores informações disponíveis em: <http://www.asis.org/Publications/ARIST/>.
[29] Bibliografia corrente, que indexa literatura da Ciência da Informação, publicada em 68 países, em 20 línguas, incluindo a língua portuguesa (BATISTA; CUNHA, 2007) .

De acordo com Araújo (2010), a partir das revisões e estudos realizados, pode-se sintetizar que:

a) os primeiros estudos de usuários da informação buscavam, então, estabelecer uma série de indicadores demográficos, sociais e humanos das populações atendidas pelas bibliotecas (ou não atendidas, no caso dos "não usuários"), mas com um foco muito particular: o levantamento de dados, como uma espécie de diagnóstico, para o aperfeiçoamento ou a adequação dos produtos e serviços bibliotecários;

b) os estudos de usuários passaram a ser utilizados, para se obter mais conhecimento sobre as [necessidades de informação do usuário] fontes, os serviços e os sistemas de informação;

c) os estudos de usuários acabam por consolidar uma tradição de pesquisas essencialmente marcadas pela ideia de uma produtividade, de uma aplicação "útil".

Assim sendo, pode-se afirmar que estudo de usuários (*user analysis, user study*) tornou-se parte relevante da CI, sendo uma das linhas de investigação que mais tem crescido nas últimas décadas.

2.4.1 Abordagens de estudos de usuários

Figueiredo (1994, p.17) observa que os "estudos de usuários são difíceis, pois devem levantar respostas lógicas, as quais possam ser interpretadas, quantitativamente, e resultar em aplicações práticas de interesse dos usuários". Na análise da autora, afloram as seguintes necessidades: criação de modelos teóricos, melhoria das metodologias adotadas e surgimento de técnicas novas.

A partir da análise de artigos sobre estudo de usuários, Dervin e Nilan (1986) identificaram duas abordagens: a **abordagem tradicional** que se caracterizava por estudos voltados ao sistema, com enfoque ao suporte ou às ferramentas (tecnologias), com dados quantitativos; e a **abordagem alternativa**, de cunho cognitivo, caracterizada por estudos centrados no usuário da informação, focando o uso da mesma em situações particulares. Figueiredo (1994), também, caracteriza estudos de usuários sob dois tipos:

a) estudos orientados ao uso de uma biblioteca ou centro de informações;

b) estudos orientados ao usuário, isto é, investigação sobre um grupo particular de usuários e como este grupo obtém a informação necessária ao seu trabalho.

A **abordagem tradicional** (orientada ao uso de uma biblioteca ou centro de informações), de acordo com Cendón e Rolim (2013), caracteriza-se por estudos voltados ao sistema,

com enfoque ao suporte ou às ferramentas (tecnologias), com dados quantitativos como número de empréstimos, de consultas, de circulação de periódicos e de análises de questões de referência. Tais estudos foram desenvolvidos a partir da percepção da necessidade da informação do público comum, da biblioteca pública ou do uso das fontes de informação de cientistas. No contexto da abordagem tradicional:

> os estudos de usuários converteram-se em ferramentas de elaboração de diagnóstico para a melhoria dos serviços – tornaram-se parte das estratégias de avaliação (de *feedback*, conforme a terminologia sistêmica tão cara ao campo): avaliação dos acervos, dos catálogos, dos periódicos, da disposição física nas estantes, dos programas de instrução bibliográfica, entre outros (LANCASTER, 2004 *apud* ARAUJO, 2010).

A segunda forma de tipificar o estudo de usuários é conhecida como **abordagem alternativa**, a qual na visão de Dervin e Nilan (1986):

> se debruçam sobre os elementos fundamentais das pesquisas sobre usos e necessidades de informação – as definições de informação e de necessidade, a natureza do uso da informação, a utilidade de diferentes abordagens para estudos do comportamento informacional, e as consequências de uso de diferentes modelos para predição.

Para Cendón e Rolim (2013), a abordagem alternativa caracteriza-se por estudos centrados no usuário da informação, com métodos de pesquisa das ciências sociais tais como: observação, entrevistas, questionários ou diários; levantamento de opiniões, pesquisa de *survey* (amostra), análise e solução de tarefas, técnica do incidente crítico, método Delphi, estudo de comunidades (grupo focal). O Quadro 4 sintetiza alguns modelos da abordagem alternativa.

Quadro 4 - Modelos teóricos da abordagem alternativa

MODELO	AUTORES	DESCRIÇÃO
Estado Anômalo do Conhecimento (ASK- *Anomalous States-of-Knowledge*)	Belkin, Oddy e Brooks (1980) Ofori-Dwumfuo	Abordou o estado que ocorre quando um indivíduo identifica uma necessidade de informação e considera seu estado de conhecimento, reconhecendo a necessidade de buscar novas informações. Essa percepção do estado inicial do conhecimento é denominada de "estado anômalo", pois pode significar lacunas de informação, incertezas e incoerências. Ao interagir com um sistema de recuperação de informações para suprir sua necessidade, o estado de conhecimento do indivíduo é constantemente alterado. No processo de busca, o usuário pode mudar sua estratégia, reavaliar suas fontes e definir o fim da busca, de acordo com suas motivações e demandas. (situação anômala > lacunas cognitiva > estratégias de busca).
Comportamento da informação (*Information Behaviour*)	Thomas D. Wilson (1981)	Transferiu o foco do estudo das fontes utilizadas para o uso da informação no ambiente do indivíduo, e compreende que a necessidade de informação é de natureza secundária e pode ser definida como fisiológica, cognitiva ou afetiva. Nesse modelo, foram utilizadas teorias de várias áreas do conhecimento e, tanto o valor da informação quanto as barreiras ao uso da informação, são concernentes ao contexto do usuário, suas demandas pessoais, profissionais e do ambiente em que está imerso.
Criação de significado (S*ense Making*)	Brenda Dervin (1983), Fraser, Edelstein, Grunig, Stamm, At-	Discutiu a criação de significado do ponto de vista da abordagem cognitiva (*sense making)*, compreendendo o indivíduo como um ser em movimento, em passagens por diversas experiências e construções de significado, mas que, diante de uma determinada situação, é obrigado a uma parada pela ausência de informação, o 'vazio cognitivo'. Identificou seis tipos de paradas de situação:

	wood, Palmour, Carter, Dewdney, Warner, Chen, Burger, Hernon.	• Decisão – qual caminho: informação pode ajudar a criar ideias; • Barreira – bloqueio no caminho: informação pode encontrar direções; • Rotatória – não se vê caminho à frente: informação pode ajudar a adquirir capacidades; • Inundação – caminho desaparecido: informação pode ajudar a obter apoio; • Problemática – arrastado para outro caminho: informação pode se tornar um elemento motivador; • Outras categorias (movimentos de entorno): Entorno perceptivo – ausência de visão: a informação pode ajudar a conectar-se com a realidade; o Entorno situacional – diversas interseções no caminho: informação pode acalmar; o Entorno social – interação entre pessoas: informação pode ser prazerosa e ajudar a atingir objetivos. (situação >lacuna cognitiva e de sentido > uso).
Valor Agregado (User-values / Value-added)	Robert S. Taylor (1986) MacMullin, Hall, Ford, Garvey, Mohr, Paisley, Farradane	O valor da informação reside no significado da informação para o ambiente do indivíduo – ambiente geográfico definido pelos limites físicos, ambiente organizacional e o ambiente social/cultural do indivíduo. A informação é buscada, porque será utilizada pelo indivíduo em uma determinada demanda que pode ser compreendida em quatro níveis de necessidade: • o nível visceral - causado pelo vazio de conhecimento; • o nível consciente - a partir do aporte de informações que permite descrever o problema; • o nível formalizado - no qual a ambiguidade é reduzida; • o nível adaptado - que representa a reelaboração da questão para processamento em um sistema de informação. O usuário dará à informação que procura diferentes usos e características tais como: descobrir 'o que' fazer ou 'como' fazer algo, descrever uma realidade, confirmar outra informação, realizar prognósticos com estimativa e probabilidade, ou outros usos para interesses de caráter motivacional, pessoal ou mesmo político. (problema _ valores cognitivos _ soluções).
Comportamento de busca de informação (*Information Search Behavior*)	David Ellis (1989)	Identificou, no processo de busca da informação, oito atividades ou características, não sequenciais, mas ainda assim interdependentes: • Início – identificar fontes de pesquisa; • Encadeamento – localizar documentos e fontes através das citações (para frente quando outras fontes relacionadas são seguidas, para trás quando fontes do documento original são seguidas); • Navegação– compilar informações gerais sobre o tema; • Diferenciação – diferenças entre as fontes servindo como filtros, analisando a qualidade do periódico, importância da autoria, por exemplo; • Monitoramento – acompanhar as informações e atualizações sobre o tema; • Extração – exploração sistemática de fontes específicas; • Verificação – verificar confiabilidade de informações e fontes; • Finalização – após certificar as fontes, verificar a correção do trabalho na literatura.
Processo de busca da informação (Information Search Process – ISP)	Carol C. Kuhlthau (1991)	As necessidades cognitivas relacionam-se com reações emocionais, ou seja, o processo de busca da informação é acompanhado por reações emocionais. O nível de incerteza é flutuante durante o processo de busca da informação (princípio de incerteza) e pode ser observado em seis estágios, divididos em três campos de experiência: emocional, cognitivo e físico. • O estágio de iniciação, quando há o reconhecimento da necessidade de informação; • O estágio de seleção no trabalho de delimitar o campo ou tema de investigação; • O estágio de exploração dos documentos acerca do tema, levando a uma expansão do tema geral (por exemplo, a leitura das fontes secundárias); • O estágio de formulação no qual ocorre o estabelecimento de foco ou perspectiva do problema; • O estágio de coleta por meio da interação com sistemas e serviços de informação para a reunião de informações; • O estágio de apresentação, o 'fim' da busca e 'solução' do problema. As etapas podem ser visualizadas a partir do caráter dinâmico do processo de busca da informação, pois neste processo há construção de conhecimento e

		significado. A formulação de um foco de interesse afeta o processo de busca, pois, para se estabelecer o foco, é preciso interpretar as informações existentes. A natureza da informação encontrada altera a posição do usuário, pois, se a informação redundante pode gerar aborrecimento, uma nova informação pode exigir uma reconfiguração de conhecimentos não disponíveis, causando ansiedade. A atitude do usuário influencia o resultado da busca, pois sua busca implica escolhas pessoais e o interesse aumenta à medida que o foco é definido e a pesquisa avança.

Fonte: adaptado de Cendón e Rolim (2013), Miranda (2007), Wilson (1999)

Na busca constante pelo aperfeiçoamento, outro movimento teórico, articulado em escala mundial, se dá com a progressiva instalação do "paradigma social" no âmbito da CI. O marco histórico desse paradigma é o I CoLIS – *International Conference on Conceptions of Library and Information Science,* realizado em 1991, na Finlândia. Neste congresso, pesquisadores de todo o mundo apresentaram diversos trabalhos, questionando os modelos teóricos até então em voga na CI e expondo propostas de novos caminhos de pesquisa (ARAUJO, 2010). Capurro (2003) argumenta que

> a ciência da informação nasce em meados do século XX com um paradigma físico, questionado por um enfoque cognitivo idealista e individualista, sendo este por sua vez substituído por um paradigma pragmático [paradigma cognitivo] e social ou [...] epistemologia social (*social epistemology*), mas agora de corte tecnológico digital.

Araújo (2010) comenta que os três paradigmas (físico, cognitivo e social), propostos por Capurro, constituem uma importante chave para a compreensão tanto da Ciência da Informação como um todo, quanto para suas subáreas de pesquisa, como o estudo de usuários. Tendo como ponto de partida o paradigma social, o autor apresenta um modelo teórico para a abordagem interacionista, onde determinadas perspectivas como a Fenomenologia, o Interacionismo Simbólico e a Etnometodologia[30] surgem como proporcionadoras de categorias e instrumentos para a pesquisa e construção da nova abordagem. Nesse contexto, o autor propõe:

> nova agenda de pesquisa para os estudos de usuários: em vez de buscar taxas de uso de determinada fonte de informação ou da frequência a uma biblioteca, torna-se essencial entender por que se usa tal fonte, que significado ela possui para quem a usa, que significado tem o acesso à biblioteca que possa explicar a frequência de consulta a ela.

Na opinião de Capurro (2003), no que tange aos estudos de usuários, o paradigma social aperfeiçoará a constituição social das "necessidades dos usuários", dos "arquivos de co-

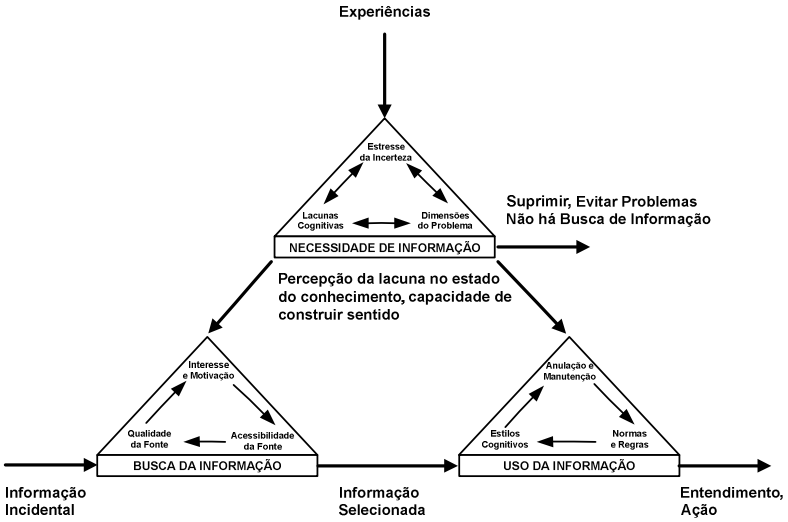
[30] Fenomenologia: concentra-se nos detalhes concretos do que acontece entre indivíduos na vida diária, diferenciando-se dessa maneira do foco mais amplo em sistemas sociais; Interacionismo Simbólico: corrente de estudos que se apoiam em três pressupostos: de que os seres humanos agem no mundo em relação aos significados oferecidos; de que esses significados são provocados pelas interações; e de que os significados são manipulados por um processo interpretativo; e Etnometodologia: pesquisa empírica dos métodos que os indivíduos utilizam para dar sentido e, ao mesmo tempo, realizar as suas ações de todos os dias: comunicar-se, tomar decisões, raciocinar (ARAÚJO, 2010).

nhecimentos" e dos esquemas de produção, transmissão, distribuição e consumo de informações.

Cendón e Rolim (2013) apresentam o modelo integrativo de Choo (2006) como exemplo para a abordagem interacionista, destacando que: "Choo integrou os processos de necessidade, busca e uso da informação em um modelo genérico de busca da informação". Na análise das autoras, a partir das abordagens de Dervin (cognitiva), Kuhlthau (emocional) e Taylor (situacional), Choo baseou-se em três propriedades quanto ao uso da informação: é socialmente construído, relaciona-se a um contexto situacional e é dinâmico.

O resultado do processo de busca é uma mudança no conjunto de conhecimentos do usuário, o que lhe permite criar significado ou tomar decisões. Por sua vez, essa mudança de *status* gera novas experiências e novas necessidades de informação, tornando o ciclo contínuo, conforme evidenciado na Figura 3.

Figura 3 - Modelo Integrativo de Choo



Fonte: Choo (2006)

Cabe ressaltar que a nova proposta (abordagem interacionista) não deixa de ser, em essência, "alternativa" à abordagem tradicional de estudos de usuários. O Quadro 5 consolida as abordagens de estudo de usuários supracitadas.

Quadro 5 - Abordagens, paradigmas e características dos estudos de usuários

ABORDAGEM	CARACTERÍSTICAS
TRADICIONAL	Paradigma Físico A informação é entendida como um objeto, uma entidade com existência física, que é transmitida de um emissor para um receptor. Tem suas raízes nas atividades clássicas da biblioteconomia de promover a transferência da informação em um determinado meio (suporte) a uma demanda específica de um usuário (receptor). O foco é sobre o sistema, não percebendo o usuário como indivíduo com objetivos, autocontrole e capacidade para tomar decisões.

	Usuário como ser passivo que deve entender o sistema e saber buscar o conteúdo desejado. Necessidade de informação é focada no que o sistema possui e não naquilo de que o usuário precisa. Modelos teóricos baseados na aplicação dos mesmos métodos das ciências naturais (exatas e biológicas) aos fenômenos humanos e sociais (Positivismo) que busca, por meio de variáveis objetivas e dados positivos, traçar leis sobre as fontes de informação mais utilizadas pelas pessoas, os hábitos de frequência à biblioteca e aos sistemas de informação ou o índice de satisfação dos usuários. Concepção comportamental em que se privilegia o comportamento externo, como contatos com fontes e usos de sistemas, com caráter de utilidade imediata, de aplicação prática.
ALTERNATIVA	Paradigma Cognitivo A Informação é capaz de transformar a estrutura das imagens, sendo um estímulo que altera a estrutura cognitiva do receptor. Informação vista como algo construído por seres humanos e os usuários como seres que estão constantemente construindo, como seres livres na criação de situações. O usuário da informação é entendido como sujeito cognoscente, possuidor de certos modelos mentais transformados, a partir da assimilação de determinados itens informacionais e mobilizados para o conhecimento do mundo. Necessidade de informação ocorre quando a pessoa reconhece que existe algo errado em seu estado de conhecimento e deseja resolver essa anomalia. Seu estado de conhecimento é insuficiente para lidar com a incerteza, conflito e lacunas em uma área de estudo ou trabalho. A busca da informação e seu valor se relacionam com a necessidade dessa informação de acordo com a visão e contexto real do usuário. Visão holística, pela qual os usuários devem ser compreendidos em um contexto social mais amplo, e os sistemas, como um dos elementos a que podem recorrer se quiserem informação. Principais vertentes: Valor Agregado (*user-values ou value-added*); Estado Anômalo de Conhecimento (ASK-*Anomalous States-of-Knowledge*); Processo Construtivista (*Constructive Process Approach*) e Construção de Sentido (*Sense-Making*).
INTERACIONISTA	Paradigma Social Critérios de seleção e relevância das informações são desenvolvidos socialmente, em conjunto com outros e não isoladamente. Considera também as construções sociais do sujeito, pois sua busca, seleção e valoração da informação têm origem no seu ambiente social. O usuário é ator principal e possui interesses pessoais e conhecimentos prévios. O indivíduo e sociedade se constituem reciprocamente, não são instâncias autônomas e separadas. Perspectivas que podem oferecer suporte: Fenomenológica; Interacionismo Simbólico e Etnometodologia.

Fonte: adaptado de Araújo (2010); Gasque e Costa (2010); Capurro (2003); Cendón e Rolim (2013); Miranda (2006)

Outra visão muito interessante sobre estudo de usuários, não concentrada nos trabalhos publicados em língua inglesa, é abordada por Calva Gonzáles (2007), ao definir que o comportamento do usuário é uma relação das fontes, recursos e grupos de convivência que direciona seu interesse. Nesta linha, segundo Casado (1994, p.17), "usuário é aquele indivíduo que necessita de informação para o desenvolvimento de suas atividades", podendo possuir, ou não, consciência dessa necessidade, afirmando que a realização de estudos de usuários serve, entre outros aspectos, para conhecer os hábitos e as necessidades de informação dos mesmos.

2.4.2 Necessidades de informação (NI)

No bojo da interdisciplinaridade da Ciência da Informação, deduz-se, quanto à Teoria das Relações Humanas, que “as necessidades descrevem exigências humanas básicas. [...] Essas necessidades se tornam desejos quando são dirigidas a objetos específicos capazes de satisfazê-las" (KOTLER, 2000). Ainda segundo o autor, “Informações podem ser produzidas e comercializadas como um produto. É essencialmente isso que escolas e universidades produzem e distribuem, mediante um preço, aos pais, aos alunos e às comunidades.” Chiavenato (2003) complementa, ao afirmar que a satisfação de uma ou mais necessidades é o objetivo final de um comportamento motivado, onde a necessidade gera tensão no sujeito, o que, por conseguinte, leva a um comportamento de busca da satisfação e a um equilíbrio, que tende a ser temporário, pois é interrompido por um estímulo ou incerteza, que o leva a uma "nova necessidade", formando um ciclo motivacional.

No âmbito da CI, essa perspectiva mais fenomenológica do que cognitiva foi expressa por Kuhlthau, no seu modelo Processo de Busca de Informação, representado na Figura 4.

Figura 4 - Processo de Busca de Informação

Estágios	**Tarefa apropriada**	**Sentimentos comuns a cada estágio**
Iniciação	Reconhecer a necessidade de informação	Insegurança
Seleção	Identificar um tema geral	Otimismo
Exploração	Investigar as informações sobre o tema geral	Confusão, frustração, dúvida.
Formulação	Formular o foco	Clareza
Coleta	Reunir informações pertencentes ao foco	Senso de direção, confiança.
Apresentação	Completar a busca de informação	Alívio, satisfação, desapontamento.

Fonte: Kuhlthau (1991 *apud* Choo, 2006, p.87)

O modelo sugere que o estado emocional inicial de incerteza, confusão e ambiguidade, associado à necessidade de buscar informação vai sendo substituído por confiança e satisfação à medida que se avança na busca e na hipótese de que o indivíduo está obtendo sucesso (OHTOSHI, 2013).

Wilson (1981) tipifica as necessidades informacionais em cognitivas, afetivas e emocionais e assinala a existência de ”motivos” na origem dos comportamentos informacionais. Esses "motivos" podem ser oriundos de várias exigências: da vida social (com destaque para o

papel do trabalho[31]), de saber (estado anômalo do conhecimento), de comunicação, de resolver um problema, de atingir um objetivo; independentes das necessidades físicas (dormir, comer) e da natureza humana (LE COADIC, 1996). O autor, ainda, argumenta que "necessidades e usos são interdependentes, se influenciam reciprocamente de uma maneira complexa, o que determinará o comportamento do usuário e suas práticas".

Posteriormente, ao abordar especificamente necessidades de informação, Le Coadic (1998) traça algumas características das NI:

a) traduzem um estado de conhecimento no qual alguém se encontra, quando se confronta com a exigência de uma informação que lhe falta e lhe é necessária para prosseguir um trabalho;

b) nascem de um impulso de ordem cognitiva, conduzido pela existência de um dado contexto (um problema a resolver, um objetivo a atingir) e pela constatação de um estado de conhecimento insuficiente ou inadequado;

c) são derivadas e comandadas pela realização de uma necessidade fundamental;

d) são também evolutivas e extensivas, porque mudam com o tempo, sob o efeito da exposição às diferentes informações iniciais, e são produzidas dinamicamente, gerando novas necessidades;

e) não podem estar separadas do contexto, da situação e do ambiente, que são essenciais para se estabelecer o seu diagnóstico.

Em relação à necessidade de informação, Crawford (1978 *apud* Casado, 1994, p. 24), considera como sendo “um conceito muito difícil de definir, isolar ou medir [...]”. Entretanto, percebe-se a estreita ligação com o problema a ser resolvido, com as características cognitivas do indivíduo e com o contexto sociocultural que o envolve.

Em abordagem complementar, Choo (2006) ressalta que a percepção do vazio que caracteriza as necessidades de informação depende do contexto profissional onde estão os indivíduos. Entre os aspectos capazes de influenciar a percepção do vazio, incluem-se variáveis como as atividades inerentes a uma profissão e aos problemas típicos do ambiente de trabalho. No entendimento de Choo (2006, p.99), as necessidades de informação

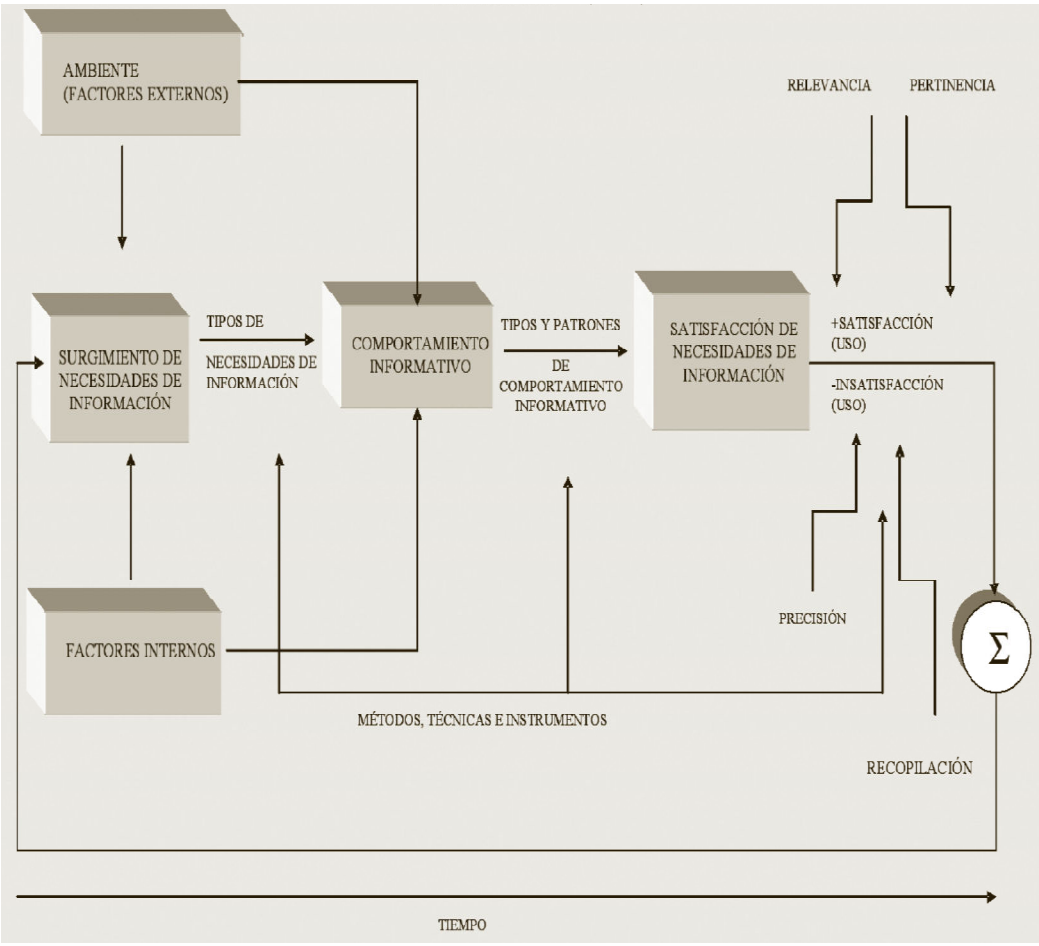
> são muitas vezes entendidas como as necessidades cognitivas de uma pessoa: falhas ou deficiências de conhecimento ou compreensão que podem ser expressas em perguntas ou tópicos colocados perante um sistema ou fonte de informação. Satisfazer uma necessidade cognitiva, então, seria armazenar a informação que responde ao que se perguntou.

[31] As características dos papéis profissionais estão conectadas com a posição ocupada, tipo de trabalho e hierarquia profissional e com a estrutura organizacional (incluindo os sistemas e serviços de informação, situação econômica, tecnologia, cultura, tradição etc.) (NIEDZWIEDZKA, 2003 *apud* MIRANDA, 2006).

Choo, também, enfatiza a existência das necessidades situacionais, ou seja, daquelas que podem surgir a partir do cotidiano das pessoas. Ressalta que a informação será considerada valiosa, se satisfizer o estado visceral de intranquilidade que originou a necessidade de informação.

Interessante notar a similaridade com que Calva Gonzáles (2007), trata do assunto, ao observar que o fenômeno das NI inclui três fases principais: o surgimento, o comportamento de busca e a satisfação das necessidades. O autor observa a necessidade de informação como um fenômeno informacional e comportamental, e apresenta o Modelo das Necessidades de Informação – Modelo NEIN, representado na Figura 5.

Figura 5 - Modelo NEIN



Fonte: Calva Gonzáles (2007)

O Modelo NEIN descreve, em três fases, as necessidades da informação pelos usuários: o surgimento da necessidade de informação do usuário, o comportamento informacional (busca da informação) e a satisfação do usuário (uso da informação), que pode ser positiva ou

não. O Modelo NEIN, também, apresenta os fatores internos e externos, os tipos de necessidades, os padrões de comportamento informacional, a valorização da satisfação, os elementos e o tempo como contribuição da necessidade informacional dos usuários da informação. Interessante notar que, satisfeitas ou não as necessidades informacionais do usuário, o modelo indica que surgem novas NI. (MARQUES; WALLIER VIANNA, 2013).

As NI são uma carência de informações sobre um fenômeno, objeto, acontecimento, ação ou feito. São produzidas por fatores externos e internos, que provocam um estado de "anomalia", motivando um comportamento para sua satisfação. Insuficiências de informação e conhecimentos geram uma NI, que surgem quando a pessoa as reconhece. A investigação das NI deve incluir a análise das características psicológicas e cognitivas do indivíduo, vinculadas à atividade que ele realiza, a todo o meio ambiente que o circunda e à sua influência sobre ele.

Miranda (2006), ao analisar a literatura sobre os estudos de NI, sintetiza que existem algumas correntes de pesquisadores que se diferenciam e se complementam pela maneira de perceber o usuário e suas necessidades:

a) alguns autores percebem o usuário por meio dos problemas que ele tenta resolver;
b) outro grupo procura captar o que esse usuário considera como anomalia no seu estado de conhecimento, diante de uma situação problemática;
c) um terceiro grupo de autores tenta entender como o usuário atribui sentido para o seu mundo, por meio da maneira como ele usa a informação.

Assim sendo, a autora sintetiza NI como um estado ou um processo no qual alguém percebe a insuficiência ou inadequação dos conhecimentos necessários para atingir objetivos e/ou solucionar problemas, sendo essa percepção composta de dimensões cognitivas, afetivas e situacionais.

2.4.3 Fontes e canais de informação

A carência informacional desencadeia uma "busca" que atenda a essa demanda. Segundo Leckie, Pettigrew e Sylvain (1996 *apud* Martinez e Oddone, 2007) existem dois fatores que influenciam, de maneira decisiva, a busca informacional:

a) Fontes de informação: locais onde são procuradas as informações. A depender do profissional e das características da informação que se busca, essas fontes variam, alterando, também, a ordem em que as fontes são consultadas. As fontes mais comumente referidas são: colegas, bibliotecas, livros, artigos e a própria experiência.

Essas fontes podem adquirir diversos formatos e ser acessadas através de diferentes canais, tanto os formais como os informais. Há fontes externas e internas, orais e escritas, pessoais e coletivas.

b) Conhecimento da informação: o conhecimento direto ou indireto das fontes, do próprio processo de busca e da informação recuperada desempenha um importante papel no sucesso da busca. Algumas variáveis, que devem ser consideradas neste sentido, são: familiaridade ou sucesso em buscas anteriores, confiabilidade e utilidade da informação, apresentação, oportunidade, custo, qualidade e acessibilidade da informação.

Barbosa (1997) constatou que uma das características mais marcantes do ambiente profissional moderno é o crescimento exponencial do número de fontes internas e externas de informação, gerando dificuldades em estabelecer uma classificação das mesmas. O autor acrescenta que, após realização de estudo sobre o uso e avaliação de fontes de informação com altos executivos em 1994, Choo classificou-as em quatro categorias conforme descrito no Quadro 6.

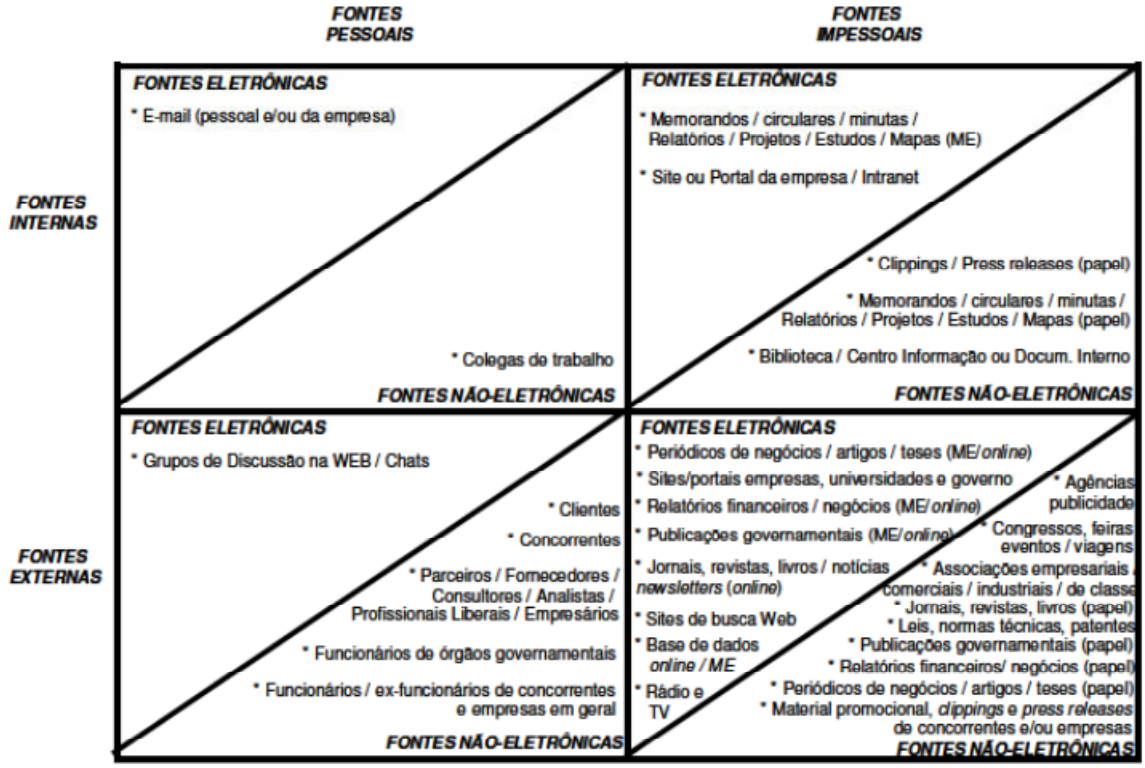
Quadro 6 - Fontes de informação organizacional

	PESSOAIS	IMPESSOAIS
EXTERNAS	Clientes Concorrentes Contatos comerciais/ profissionais Funcionários de órgãos governamentais	Jornais, periódicos Publicações governamentais Rádio, televisão Associações comerciais e industriais Conferências, viagens
INTERNAS	Superiores hierárquicos, membros da diretoria Gerentes subordinados Equipe de funcionários	Memorandos e circulares internos Relatórios e estudos internos Biblioteca da organização Serviços de informação eletrônica

Fonte: Choo (1994)

Passada uma década, Mafra Pereira e Barbosa (2008) buscam atualizar os estudos supracitados, trazendo, para o contexto contemporâneo do ciberespaço, uma classificação alternativa de fontes de informação. Essa classificação apresenta trinta espécies de fontes, descritas no Quadro 7, a partir de três critérios: origem (fontes internas ou externas), relacionamento/proximidade (pessoais ou impessoais) e mídia (fontes eletrônicas e não eletrônicas).

Quadro 7 - Classificação das fontes de informação



Fonte: Mafra Pereira e Barbosa (2008)

Cabe destacar que, ao mesmo tempo em que o Ciberespaço oferece rapidez na inserção de dados e facilidades (busca *Web*, correio eletrônico, mídias eletrônicas, grupo de discussão etc.), não assegura aos usuários qualidade e confiabilidade das informações disponibilizadas. Cabe, pois, ao usuário sempre validar a origem e os responsáveis pela disponibilização e confecção do material pesquisado. Em relação à satisfação das necessidades de informação para a realização das tarefas cotidianas, Miranda (2006) supõe que:

> ao solucionar determinado problema ou preencher uma lacuna cognitiva, o indivíduo escolhe suas fontes de informação de acordo com o seu conhecimento prévio sobre elas, com a experiência positiva ou negativa no seu uso, e pelo resultado obtido com seu uso anterior em situações semelhantes.

Durante as fases de identificação das fontes de informação e de formulação da estratégia de busca, o usuário avalia os possíveis meios ou canais que lhe permitirão resolver seu problema, levando em consideração, sejam eles humanos ou computadorizados, sua acessibilidade e usabilidade (LE COADIC, 2004). Em consonância, Choo (2006), também, ressalta que a acessibilidade é fator que rege a seleção de um canal (mensurada pelo esforço e tempo despendido por um indivíduo para acessar a informação em um dado sistema), bem como a qualidade da informação disponibilizada. O autor acrescenta que o ambiente de trabalho, por sua vez, pode afetar decisivamente o modo como os canais de informação são selecionados e

usados em uma organização. Para Le Coadic (2004), um canal de informação deve ser construído de forma coerente com os usos dados à informação e os respectivos efeitos dos mesmos nas atividades organizacionais. As interações de busca em canais de informação podem ocorrer:

a) no modo pessoa-pessoa, quando existe uma comunicação direta (pessoal, telefone e reuniões);

b) entre indivíduos ou grupos;

c) no modo pessoa-computador, quando um usuário opta por utilizar um sistema de informação computadorizado, para buscar a informação de que necessita;

d) na interação pessoa-computador-pessoa, possibilitada atualmente pela rede mundial de computadores e pelos serviços suportados pela mesma, como: correios eletrônicos, mídias sociais, conferências eletrônicas e trabalho colaborativo. [32]

Outra forma de tipificar os canais de informação é classificá-los em **formais -** onde as informações são registradas e disseminadas de forma impressa, através de fontes primárias e secundárias, e **informais** - onde as informações são transmitidas diretamente, pessoa a pessoa, através de contatos interpessoais, telefonemas, cartas e reuniões científicas (MEDEIROS, 1984 *apud* CAVALCANTI e CUNHA, 2008).

2.4.4 Comportamento informacional

Como pôde ser percebido anteriormente, o tema **comportamento informacional** vem substituindo a nomenclatura "necessidades e usos da informação" nos trabalhos apresentados nas últimas décadas no ARIST (Quadro 3, p. 31). Em relação ao ARIST, ao analisar as mudanças de foco ocorridas, Gasque e Costa (2010) consideram os seguintes pontos na evolução dos estudos de comportamento informacional:

a) pesquisas mais centradas no indivíduo;

b) inclusão de outros grupos estudados, além de cientistas e tecnólogos;

c) abordagem multifacetada, englobando os aspectos sociocognitivo e organizacional;

d) compreensão do comportamento informacional como processo em que os indivíduos estão, constantemente, buscando e usando informações;

e) ampliação dos estudos qualitativos, assim como do uso de múltiplos métodos;

[32] Também chamados de fontes pessoais de informação, particularmente os serviços de correio eletrônico, as listas e grupos de discussão são usados para enviar e receber mensagens entre indivíduos e grupos de pessoas, facilitando e agilizando o processo de comunicação informal entre especialistas (CENDÓN, 2000).

f) maior consistência teórica com aumento de fundamentação interdisciplinar;

g) crescimento do número de pesquisas, em todas as partes do mundo.

Ainda em relação a comportamento informacional, Gasque e Costa (2010, p.31) esclarecem que:

> a evolução conceitual dos 'estudos de usuários' para 'estudos de comportamento informacional' reflete a necessidade de se compreenderem os processos em uma perspectiva multidimensional. Isso porque ocorre profunda imbricação na tessitura dos fenômenos, em que vários fatores desempenham papéis decisivos na produção do conhecimento.

Para Davenport (1998, p.110), comportamento informacional "se refere ao modo como os indivíduos lidam com a informação". Isto inclui a busca, o uso em suas diversas formas e até mesmo o ato de ignorar a informação. Wilson (2000b) acrescenta que o comportamento informacional pode ser definido como a totalidade do mesmo em relação a fontes e canais de informação, incluindo a busca passiva e ativa, bem como o uso de informação.

Não obstante, os ambientes sociais e organizacionais, que envolvem o usuário, afetam significativamente a motivação individual, os usos da informação e seus fluxos. Nesse sentido, Pettigrew et al. (2001 *apud* Miranda, 2006) definiram o tema "comportamento informacional", como sendo a forma pela qual as pessoas necessitam, buscam, fornecem e usam a informação em diferentes contextos, incluindo o espaço de trabalho e a vida diária.

Para Wilson (2000b), o uso da informação consiste nos atos físicos e mentais relacionados à incorporação da informação encontrada junto à base de conhecimentos existentes do indivíduo. Taylor (1996 *apud* Choo, 2006, p.105) propõe oito categorias de uso da informação:

a) esclarecimento: a informação é usada para criar um contexto ou dar um significado a uma situação;

b) compreensão do problema: a informação é usada de uma maneira mais específica, para permitir a compreensão de um determinado problema;

c) instrumental: a informação é usada para que o indivíduo saiba o que e como fazer. As instruções são uma forma comum de informação instrumental;

d) factual: a informação é usada para determinar os fatos de um fenômeno ou acontecimento;

e) confirmativa: a informação é usada para verificar outra informação;

f) projetiva: a informação é usada para prever o que vai acontecer no futuro;

g) motivacional: a informação é usada para iniciar ou manter o envolvimento do indivíduo;

h) pessoal ou política: a informação é usada para criar relacionamentos ou promover uma melhoria de *status*, de reputação ou de satisfação pessoal.

O uso da informação é a seleção e o processamento das informações que resultam em novos conhecimentos ou ações. A informação é usada para responder a uma questão, solucionar um problema, tomar uma decisão, negociar uma posição ou dar sentido a uma situação. Na metáfora transpor o vazio/criar significado, o uso da informação é visto com uma ajuda que o indivíduo deseja de informação, para continuar, e as trajetórias de vida (OHTOSHI, 2013).

As pesquisas de comportamento informacional estão em contínua expansão. Case (2006) categoriza tal comportamento, ao afirmar que a maior parte das pesquisas sobre o tema está dividida entre três abordagens: por ocupação/profissão, por papel social ou por grupos demográficos (idade, gênero, grupos étnicos), sendo a abordagem voltada para a ocupação predominante. De acordo com o autor, no que se referem à abordagem ocupacional, diversas pesquisas já foram realizadas, com sucesso, sobre o comportamento informacional de engenheiros, cientistas, pesquisadores da área de Humanidades, gerentes, entre outros, podendo ser agrupadas conforme a sua orientação para tarefas ou não, bem como quanto às pessoas ou aos sistemas.

Gasque e Costa (2010) afirmam que os indivíduos se engajam nas ações de busca, uso e transferência de informação, quando dela têm necessidade. Portanto, o comportamento informacional, compreendido como processo natural do ser humano no papel de aprendiz da própria vida, requer visão ampla do pesquisador, exigindo o entendimento das relações estabelecidas em determinado espaço-tempo em que ações supracitadas ocorrem.

2.5 Considerações finais

Neste capítulo, buscou-se a aproximação do entendimento de Alves (1992, p. 56), quando afirma que

> a literatura revista deve formar com os dados um todo integrado: o referencial teórico servindo à interpretação e as pesquisas anteriores orientando a construção do objeto e fornecendo parâmetros para comparação com os resultados e conclusões do estudo em questão.

A principal finalidade da revisão anteriormente realizada foi embasar a definição das metodologias mais adequadas à análise do comportamento informacional dos profissionais que atuam na segurança cibernética da Administração Pública Federal. Os tópicos abordados,

norteados pelos objetivos específicos da pesquisa, favoreceram as escolhas da abordagem teórica, o método a ser empregado e os procedimentos de coleta de dados.

Conceitos e pontos de vista foram consolidados, como a proposta do autor de que a segurança cibernética insere-se no contexto mais abrangente da segurança da informação. Tal assertiva foi ratificada pela recente norma ISO/IEC 27032 (ao abordar o relacionamento entre segurança cibernética e os demais domínios da Segurança), bem como pela definição de gestão de SIC, proposta pelo GSIPR, no âmbito da APF.

No desenvolvimento desta pesquisa, torna-se fundamental considerar, além das características cognitivas e dos fatores emocionais, o aspecto situacional, ou seja, o ambiente (de trabalho) onde as necessidades, a busca e o uso da informação ocorrem. Particular atenção foi destinada ao papel dos agentes públicos, a complexidade do ambiente cibernético da instituição e as características dos problemas oriundos das atividades típicas realizadas, tais como: a correção das vulnerabilidades de segurança nos sistemas de informatizados, a mitigação das ameaças ou o tratamento e a resposta aos incidentes de segurança nas redes de computadores. De igual forma, também, percebe-se o alinhamento da pesquisa com:

a) a definição do "objeto" da CI por Capurro (2003), como sendo "uma integração da perspectiva [...] do paradigma cognitivo dentro de um contexto social [APF] no qual diferentes comunidades desenvolvem seus critérios de seleção e relevância";
b) a abordagem ocupacional proposta por Case (2002), na medida em que foram selecionados, para análise, profissionais evolvidos diretamente com o gerenciamento da Segurança Cibernética.

3 METODOLOGIA

Este capítulo apresenta a metodologia desenvolvida para a realização da pesquisa, excetuando os aspectos de pesquisa bibliográfica. Inicia por apresentar o modelo conceitual adotado para a análise dos dados coletados.

3.1 Modelo Conceitual

Nessa subseção, buscaram-se selecionar, no contexto da Ciência da Informação, as abordagens e modelos na subárea de Estudo de Usuários mais condizentes com o problema da pesquisa. Assim sendo, adotou-se um modelo baseado na **abordagem alternativa** revisada na seção 2.4.1. Na abordagem alternativa de estudos de usuários, um dos aspectos mais significativos refere-se ao fato de que o núcleo dos estudos migra dos sistemas de informação para o usuário. Ao analisar a literatura sobre o tema, Gasque e Costa (2010), também, evidenciam:

a) a percepção do usuário sobre a utilidade e o valor do sistema de informação;
b) a maneira como as pessoas dão significado ao mundo e ao uso da informação nesse processo;
c) a análise de como as pessoas buscam informações relativas a situações em que seu conhecimento é incompleto.

Assim sendo, adotou-se o **Modelo de comportamento informacional de Thomas D. Wilson**, revisado em 1996. A escolha pautou-se, principalmente, pelo mesmo estar centrado nas pessoas (usuário), em seu contexto cognitivo e ambiental, e por adotar abordagem multidisciplinar na explicação do comportamento informacional.

Inicialmente, Wilson (1981) propôs seu modelo de necessidades e buscas de informação, no início da década de 1980, levando em consideração o ambiente, o papel social e as necessidades físicas, afetivas e cognitivas pessoais. Posteriormente, o autor revisa sua proposta, ao afirmar que um modelo de estudo de usuário deve começar com uma modelagem da organização em que ele trabalha e com o entendimento de como isso afeta o comportamento individual na busca, uso e transferência da informação.

Continuando e aprimorando o seu trabalho, Wilson desenvolve um novo modelo geral de comportamento informacional, onde compara e relaciona seu desenho de necessidades e buscas de informação de 1981 com outros modelos, tais como: a Teoria da criação de significado (S*ense Making*) de Brenda Dervin, o modelo de Comportamento de busca de informação

(*Information Search Behavior*) de David Ellis e o modelo de Processo de busca da informação (*Information Search Process – ISP*) de Carol C. Kuhlthau (WILSON, 1999, 2000a).

Em relação ao comportamento informacional, Wilson (2000b) propõe quatro definições básicas:

a) comportamento informacional: a totalidade do comportamento humano em relação ao uso de fontes e canais de informação, incluindo a busca da informação passiva ou ativa;

b) comportamento de busca da informação: a atividade ou ação de buscar informação em consequência da necessidade de atingir um objetivo específico;

c) comportamento de pesquisa de informação: o nível micro do comportamento, em que o indivíduo interage com sistemas de informação de todos os tipos, levando em consideração tanto a interação homem-máquina (uso de *mouse*, teclado e outros dispositivos do computador) como o ponto de vista intelectual (seleção de expressões booleanas ou de outras estratégias para obtenção de informações e o julgamento da relevância dos dados ou informações obtidas);

d) comportamento do uso da informação: é considerado o passo seguinte ao comportamento de busca e pesquisa da informação. Constitui-se num conjunto dos atos físicos e mentais, que envolve a incorporação, aos conhecimentos prévios do indivíduo, da nova informação encontrada e julgada relevante.

No que tange à busca da informação, Wilson (1997) apresenta um conjunto de oito itens *(Intervening variables*) os quais intervêm no processo de busca informacional:

a) características pessoais - dissonância cognitiva e exposição seletiva;

b) variáveis emocionais e psicológicas - tendência à curiosidade ou aversão ao risco;

c) variáveis educacionais - nível de escolaridade e bases de conhecimento;

d) variáveis demográficas - idade e sexo;

e) variáveis sociais ou interpessoais - função exercida no trabalho (gerente, analista, técnico etc.);

f) variáveis de meio ambiente - localização geográfica, diferenças culturais e tempo disponível;

g) variáveis econômicas - recursos de TIC disponíveis e custo (tempo/recursos) da busca;

h) características relativas às fontes - acessibilidade, credibilidade e canais de comunicação das fontes de informação.

No modelo de comportamento da informacional (*Human Information Behavior*), revisado de Wilson, é fundamental considerar não só a inter-relação das pessoas envolvidas, das tarefas laborais, dos mecanismos de ativação (*Activating mechanism*) e das variáveis que intervêm no processo de busca informacional *(Intervening variables*), bem como a presença de três ideias teóricas relevantes:

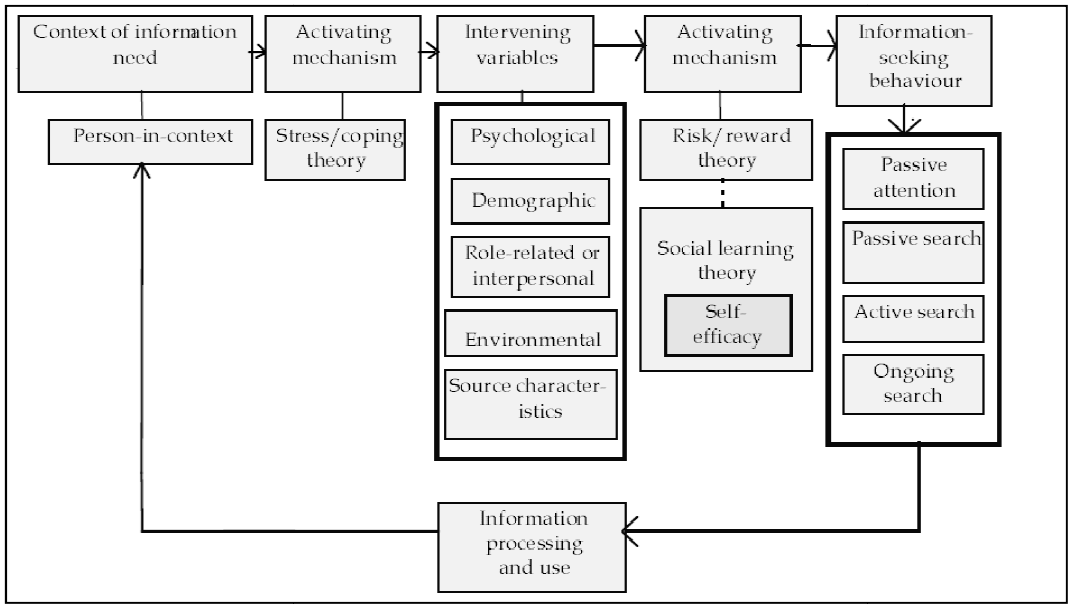
a) a teoria do estresse/enfrentamento (*stress/coping theory*) - busca explicar por que algumas "necessidades" não ocasionam um comportamento de busca da informação;

b) a teoria do risco/recompensa (*risk /reward theory*) - ajuda a esclarecer o motivo pelo qual uma pessoa utiliza uma fonte de informação em detrimento de outras;

c) a teoria da aprendizagem social (*social learning theory*) - incorpora o conceito de "autoeficácia", em que qualquer indivíduo pode produzir, com sucesso, o comportamento necessário à obtenção dos resultados por ele desejados.

Os aspectos supracitados estão inseridos no Modelo, que é estruturado em três módulos: Contexto da necessidade de informação (*Context of information need*), Comportamento de busca da informação (*Information seeking behaviour)* e Processamento e uso da informação (*Information processing and use*), conforme detalhado na figura 6.

Figura 6 - Modelo de comportamento informacional de Wilson



Fonte: Wilson (1997, p.569)

O Modelo revisado de Wilson passou a assumir caráter cíclico, que se inicia (lado superior esquerdo) com as necessidades de informação percebidas pelo usuário inserido em um

contexto (*Context of information need*). Em seguida, são acionados mecanismos de ativação (*Activating Mechanism*) que atuam diretamente na busca (ou não) da informação pela pessoa.

No bojo dos mecanismos de ativação, encontram-se:

a) o estresse e as formas de lidar com ele;

b) a percepção da recompensa (os esforços da pesquisa são proporcionais aos benefícios por cada fonte);

c) o risco diante da possibilidade de cometer erros ou de responder insatisfatoriamente às expectativas;

d) a existência da crença conhecida com Autoeficácia (*Self-efficacy).*

Os mecanismos de ativação são intercalados pelas variáveis intervenientes (*Intervening variables*) mencionadas anteriormente. Na sequência, a pessoa pode adotar diferentes tipos de comportamento de busca da informação (*Information seeking behaviour)*, tais como:

a) atenção passiva: forma não intencional de adquirir informação, como ouvir rádio ou assistir a programas de televisão [ou ainda navegar pela Internet];

b) busca passiva: significa a ocasião quando um tipo de busca (ou outro comportamento) resulta na aquisição de informação, a qual passa a ser relevante para a pessoa;

c) busca ativa: tipo de busca mais comum encontrada na CI, em que a pessoa busca, ativamente, a informação de que necessita (detalhadas nos Modelos de Ellis e Kuhlthau);

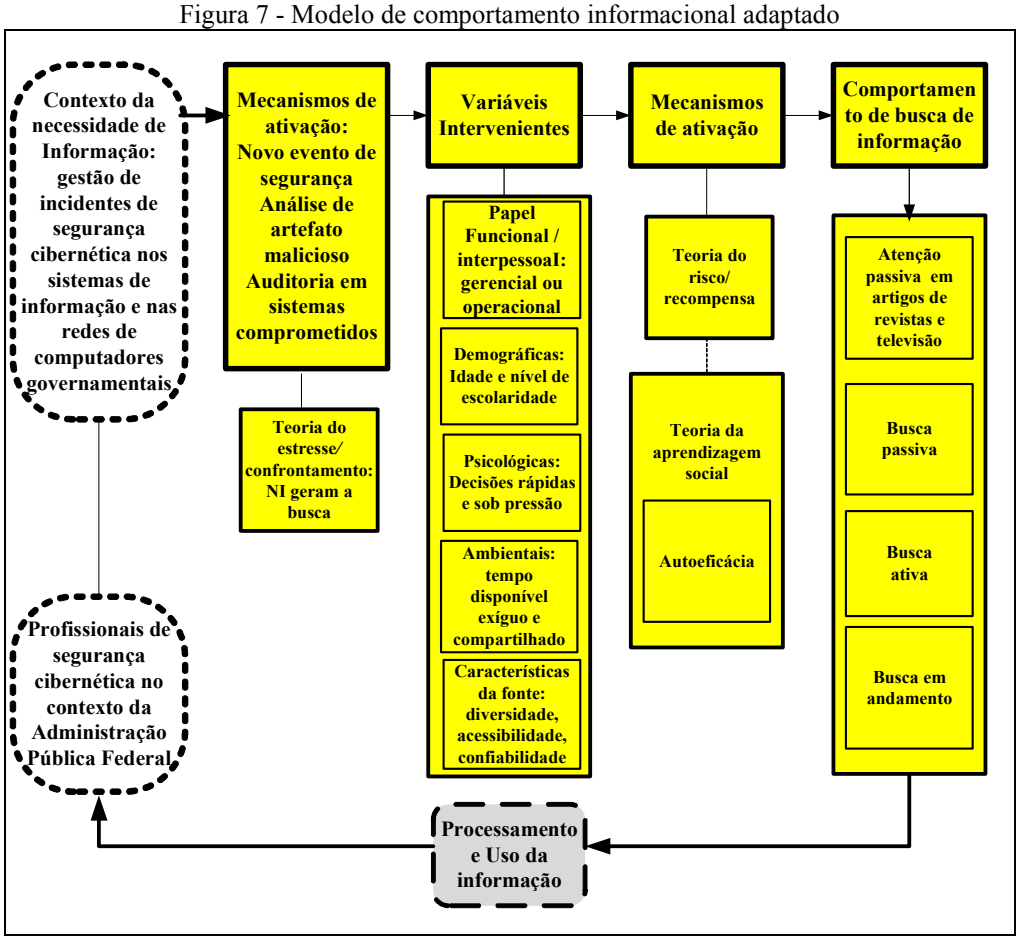
d) busca em andamento: a busca ativa está estruturada, somente, no campo das ideias, crenças e valores.

Por fim, na etapa "processamento e uso da informação" (*Information processing and use*), a informação é avaliada quanto ao seu efeito sobre a necessidade percebida, a qual pode ser satisfeita ou não, tornando o modelo cíclico, ou seja: o modelo pode se repetir enquanto a necessidade não for satisfeita.

3.2 Modelo de Comportamento Informacional Adaptado

Baseado no Modelo de comportamento informacional de Thomas D. Wilson de 1996, a Figura 7 ilustra um Modelo de comportamento informacional adaptado ao presente estudo.

Figura 7 - Modelo de comportamento informacional adaptado



Fonte: adaptado de Wilson (1997)

O modelo da Figura 7 preserva a estrutura de três módulos de Wilson. No primeiro módulo, o contexto das necessidades de informação abrange os profissionais responsáveis pela gestão da segurança cibernética na APF, no caso da pesquisa, os agentes públicos que realizaram o CEGSIC. O segundo módulo inicia-se com os mecanismos de ativação, que, no caso, podem ser: uma demanda envolvendo um novo evento de segurança, a análise de artefato malicioso ou a auditoria em sistemas comprometidos. Inserem-se, nesta etapa, as variáveis intervenientes (com ênfase no papel funcional) e o comportamento de busca de informação. Finalmente, o terceiro módulo refere-se ao uso da informação pelo agente público, com a finalidade de atender a uma demanda dentro do seu ambiente de trabalho e de acordo com os papéis desempenhados na organização. Os procedimentos metodológicos e os instrumentos de coleta de dados aplicados ao modelo proposto estão detalhados na seção 3.4.

Dessa forma, o modelo de Wilson, adotado e customizado de acordo com a temática da pesquisa, contempla o objetivo da mesma: analisar o comportamento informacional dos agentes públicos que atuam no contexto da gestão da segurança cibernética no ambiente da Administração Pública Federal. Não obstante, o modelo adaptado considera as afirmações

basilares que vêm sendo discutidas ao longo do trabalho. Essas questões norteadoras do presente estudo, chamados de pressupostos, são consolidadas a seguir.

3.3 Pressupostos

3.3.1 Pressuposto Geral

Para analisar o comportamento informacional na gestão da segurança cibernética da Administração Pública Federal, é preciso considerar o contexto situacional, bem como o comportamento de busca e uso da informação do agente público nas atividades relacionadas à segurança do espaço cibernético.

3.3.2 Pressupostos Específicos

Os três pressupostos específicos para a realização do trabalho foram:

a) o contexto situacional está diretamente relacionado com o papel desempenhado, na organização, pelo agente público que atua na segurança cibernética. Considera-se que o papel desempenhado assuma uma das três perspectivas de atuação: nível estratégico (coordenação, planejamento e gestão de alto nível), nível operacional (atuação direta com sistemas computacionais, de controle ou rede de computadores) ou nível tático (ações de resposta a incidentes de segurança em redes de computadores); [33]

b) a análise do comportamento de busca é caracterizada pelas fontes e pelos canais utilizados no atendimento das necessidades de informação. A pesquisa, não faz distinção entre fontes eletrônicas e não eletrônicas, mas considera, separadamente, canais/fontes pessoais (informais) ou impessoais (formais), bem como externas ou internas à organização;

c) as tarefas diárias desempenhadas no ambiente de trabalho influenciam o uso da informação. Na presente pesquisa, as tarefas executadas estão relacionadas ao papel desempenhado no ambiente de trabalho.

[33] Os papéis desempenhados, na organização, pelos agentes públicos que atuam na segurança cibernética, caracterizados nesses três perfis (estratégico, operacional e tático), bem como os procedimentos realizados por esses agentes quanto à gestão da segurança da Informação no espaço cibernético da APF podem ser consultados no artigo: O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos (WALLIER VIANNA; FERNANDES, 2014).

O Quadro 8 correlaciona os pressupostos específicos (PE), suas variáveis e as questões do instrumento de coleta quantitativo.

Quadro 8 - Relacionamento entre os PE e o instrumento de coleta de dados

PRESSUPOSTOS ESPECÍFICOS	VARIÁVEIS	BLOCO DE QUESTÕES
O contexto situacional está diretamente relacionado com o papel desempenhado, na organização, pelo agente público que atua na segurança cibernética	• nível estratégico • nível operacional • nível tático	A.7 a A.8
A análise do comportamento de busca é caracterizada pelas fontes e pelos canais utilizados no atendimento das necessidades de informação	•relevância •confiabilidade •acessibilidade	B.1 a B.17
As tarefas diárias desempenhadas no ambiente de trabalho influenciam o uso da informação.	•frequência •pertinência	C.1 a C.7

Fonte: elaboração própria

3.4 Procedimentos Metodológicos

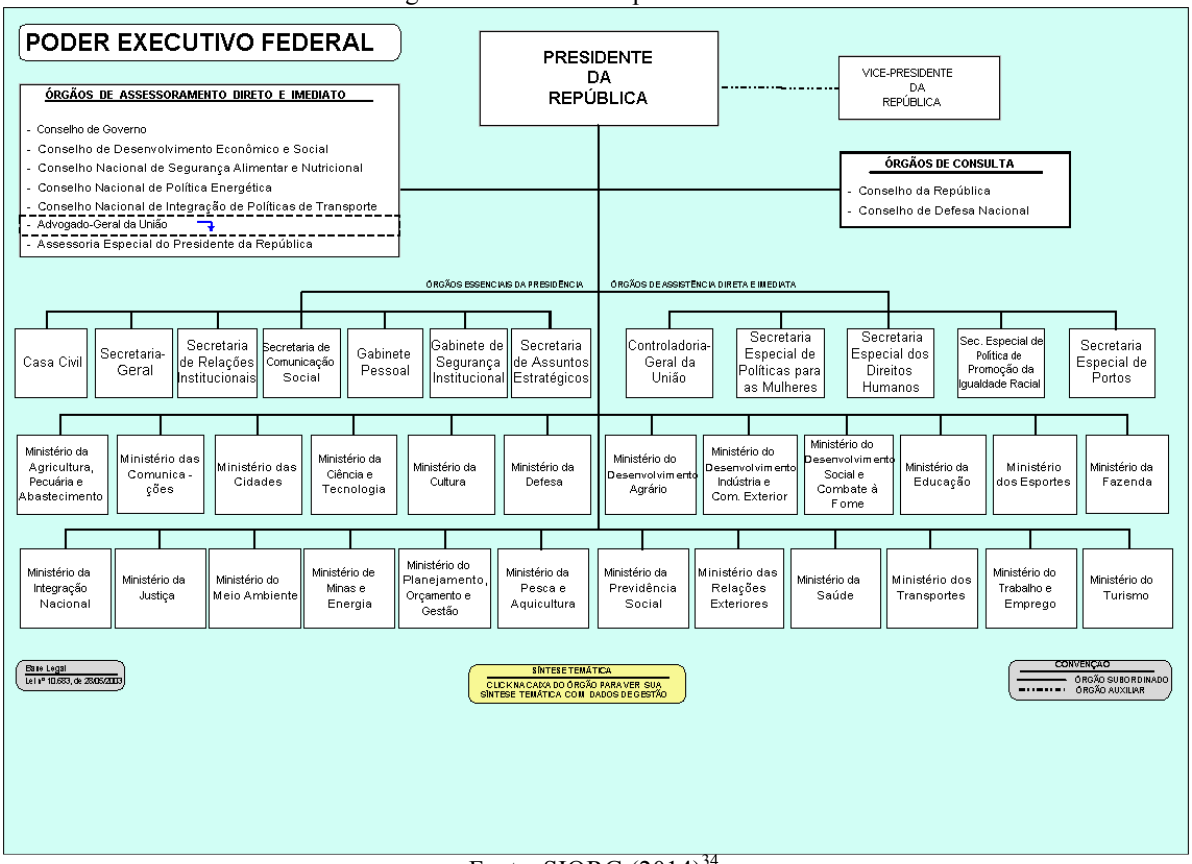
3.4.1 Contexto da pesquisa

A fim de atingir os objetivos desejados, a pesquisa foi desenvolvida no contexto da Administração Pública Federal, junto a indivíduos que atuam, diretamente, no contexto da segurança cibernética governamental brasileira.

3.4.1.1 Administração Pública Federal (APF)

Foi escolhido, como universo, os servidores e empregados de órgãos e entidades do Poder Executivo, conhecido como Administração Pública Federal (APF). O grande número de entidades da APF (como pode ser observado na Figura 8); as imensas diferenças na qualificação de pessoal, nas práticas e nas políticas já estabelecidas; os diversos níveis de segurança implementados; a localização geográfica diversificada no território nacional e muitos outros fatores, inclusive os de natureza política, oferecem um contexto rico e abrangente da realidade do e-gov brasileiro. (WALLIER VIANNA, 2011).

Figura 8 - Estrutura do poder executivo



Fonte: SIORG (2014)[34]

Cabe destacar que a APF oferece diversificados serviços que podem ser acessados, a qualquer tempo e lugar, por diversos dispositivos, desde computadores até aparelhos móveis, como telefones celulares.

3.4.1.2 CEGSIC

A amostra foi selecionada dentre os servidores e empregados concludentes e alunos do Curso de Especialização em Gestão da Segurança da Informação e Comunicações (CEGSIC). A amostragem utilizada, baseada nos alunos e concludentes do CEGSIC, pode ser classificada como não probabilística, do tipo por tipicidade ou intencional. Ressalta-se que a escolha foi realizada intencionalmente com base na acessibilidade e na conveniência dos participantes. Esta forma de amostragem consiste em selecionar um subgrupo da população que, com base nas informações disponíveis, possa ser considerado representativo de toda a população (GIL, 2008).

[34] Disponível em: <http://www.siorg.gov.br/Presidencia/PRESIDENCIA_HL_frame.htm>. Acesso em: 02 mar. 2014.

O CEGSIC foi, inicialmente, criado sobre demanda do Gabinete de Segurança Institucional da Presidência da República (GSIPR). O Curso em questão é realizado pela Universidade de Brasília (UnB) que recebe colaboração, apoio e aporte de recursos organizacionais e financeiros do GSIPR. Na sua criação, a finalidade do CEGSIC foi aperfeiçoar as competências necessárias para desenvolver metodologias de gestão de Segurança da Informação e Comunicações, aplicáveis a organizações públicas. Seu público alvo são os servidores públicos federais executivos civis ou militares, ou seja, pertencentes à APF (FERNANDES, 2012a).

O curso teve início em 2007 com uma turma presencial. A partir de 2009, o CGESIC passou a ser realizado na modalidade de Ensino à Distância (EaD), na forma semipresencial. O curso é dirigido exclusivamente aos que integram o quadro de recursos humanos de órgão ou entidade do poder executivo federal, civis ou militares, em exercício de atividade em caráter permanente ou com contrato de trabalho por tempo indeterminado, cujo órgão ou entidade pública de origem e lotação é do poder executivo federal brasileiro. Assim sendo, o CEGSIC complementa a formação de agentes públicos, detentores de formação de nível superior em qualquer área do conhecimento, visando ao aperfeiçoamento de habilidades e competências para a gestão da segurança da informação e da segurança cibernética, em órgãos e entidades da APF (CEGSIC 2012/2014, 2013).

3.4.2 Pesquisa Descritiva, de Método Misto e Modelo Explanatório

Quanto à sua finalidade, a presente pesquisa caracteriza-se como descritiva. Segundo Moresi (2003), realiza-se esse tipo de investigação para descrever as características de determinada população ou de determinado fenômeno. No entendimento de Cervo, Bervian e Silva (2007), a pesquisa descritiva observa, registra, analisa e relata fatos ou fenômenos sem manipulá-los. Busca, também, conhecer situações do comportamento humano, cujo registro não consta de documentos. Em complemento, os autores indicam que, para viabilizar a operação de coleta de dados em uma pesquisa descritiva, são utilizados, como principais instrumentos: a observação, a entrevista, o questionário e o formulário.

Baptista e Cunha (2007, p.182) consideram que as metodologias de pesquisa devem ser usadas de acordo com o tipo de pesquisa a ser desenvolvida. Segundo os autores, alguns problemas "pedem" uma abordagem qualitativa, outros uma abordagem quantitativa, por exemplo, quando há conjuntos de pessoas com hábitos semelhantes por área de conhecimento, enfatizando-se que não é a metodologia que determina a pesquisa e, sim, o problema que se pretende resolver.

Assim sendo, desenvolveu-se o presente projeto em duas etapas distintas, por meio de dois instrumentos, nomeadamente: análise bibliográfica e levantamento. A análise bibliográfica consiste no uso de fontes das quais serão coletados dados (conceitos) sobre segurança da informação na APF, segurança cibernética e estudos de usuários (modelos de comportamento informacional), bem como sobre as características do espaço cibernético. O levantamento, por sua vez, consiste na aplicação de questionários e de entrevistas em profundidade (*in depth interview*) com amostras do universo investigado (CEGSIC).

Dessa forma, a segunda etapa da presente pesquisa caracterizou-se pela estratégia de investigação **mista** na qual se adotam abordagens tanto qualitativas como qualitativas.[35] Na abordagem quantitativa, o pesquisador coleta dados em um instrumento que mede atitudes, sendo as informações analisadas por meio de procedimentos estatísticos. Na abordagem qualitativa, o pesquisador coleta elementos significativos do ponto de vista dos participantes, concentrando-se em um único fenômeno ou conceito (CRESWELL, 2007). De acordo como Creswell e Clark (2007), os quatro principais modelos (*designs*) para execução de pesquisas, utilizando-se métodos mistos, são:

a) Triangulação;

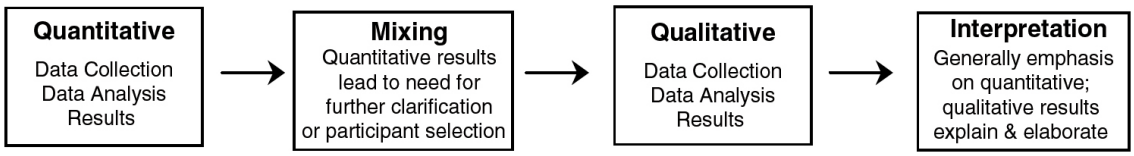
b) Explanatório;

c) Exploratório;

d) Transformativo (ou embutido).

No caso desta pesquisa, adotou-se o modelo Explanatório representado na Figura 9.

Figura 9 - Modelo Explanatório



Fonte: Creswell e Clark (2007)

De acordo com Creswell (2007), a estratégia do modelo explanatório é sequencial, ou seja, é caracterizada pela coleta e pela análise de dados quantitativos, seguida de coleta e análise de dados qualitativos, que são desenvolvidas sobre os resultados quantitativos inicialmente levantados. Assim sendo, neste estudo, foi utilizada a estratégia explanatória sequencial em duas fases:

[35] "São os tipos projetos ou modelos qualitativos, quantitativos e de métodos mistos que proporcionam uma direção específica aos procedimentos em um projeto de pesquisa" (CRESWELL, 2007).

a) Na primeira fase, foi realizado um levantamento amplo para generalizar os resultados de uma população, por meio da aplicação de um questionário a todos os alunos do CEGSIC;
b) Após a análise dos dados quantitativos levantados, entrevistou-se uma parcela dos alunos do CEGSIC, a fim de se obter uma visão detalhada dos conceitos/aspectos levantados no questionário, bem como o aprofundamento do entendimento do problema da pesquisa.

Minayo (2007) acrescenta que o levantamento inclui, não somente o método e as características próprias do pesquisador, mas também os instrumentos da operacionalização do conhecimento (técnicas), os quais serão detalhados nas subseções que se seguem.

3.4.3 Instrumentos de Coleta dos Dados

3.4.3.1 Questionário

O instrumento base da coleta de dados foi o questionário. O mesmo foi aplicado nos alunos e concludentes do CEGSIC, desde a sua criação tanto no modelo presencial, quanto na modalidade Ensino à Distância (EaD), incluindo a atual turma 2012/2014.

De acordo com Cavalcanti e Cunha (2008), o questionário consiste numa lista de questões a serem propostas pelo pesquisador junto aos informantes, para obtenção de dados, escolhidos pelos mais diversos métodos de amostragem. Brantley (2006) esclarece os três objetivos específicos do mesmo: em primeiro lugar, traduzir a informação desejada em um conjunto de questões específicas que os questionados tenham condições de responder; em seguida, motivar e incentivar o questionado a se deixar envolver pelo assunto, cooperando e completando a série de questões; e em terceiro lugar, o questionário deve sempre minimizar o erro na resposta.

Cunha (1982) lista as seguintes vantagens de um questionário:

a) é um método rápido em termos de tempo, porque estipula-se uma data para a devolução dos questionários preenchidos;
b) é barato, porque o custo das tarifas postais [correio eletrônico] para a remessa dos questionários é menor do que o custo de salários a serem pagos a entrevistadores;
c) pode-se atingir, ao mesmo tempo, uma grande população dispersa numa ampla região geográfica;

d) proporciona maior grau de liberdade e tempo ao respondente, pois o mesmo não é constrangido pela presença do entrevistador;

e) há possibilidade de serem menores as distorções, desde que o informante não sofra a influência ou pressão do pesquisador.

Com o advento da *Word Wide Web* (WWW), o questionário passou a adquirir uma importância maior em relação aos outros instrumentos de coletas de dados. A WWW tornou mais rápida a remessa, o preenchimento e a devolução do questionário, apresentando ainda as seguintes vantagens: menor tempo para transcrição das respostas, para a tabulação e análise estatística, e enormes perspectivas para o envio personalizado dos resultados aos respondentes, o que poderá estimular a oportunidade de uma participação futura (BAPTISTA; CUNHA, 2007, p.178).

De forma geral, procurou-se seguir os passos propostos por Brantley (2006), na elaboração do questionário:

a) especificar a informação de que necessitamos;

b) especificar o tipo de método da entrevista;

c) determinar o conteúdo das perguntas individuais;

d) planejar as questões de modo a superar a incapacidade e/ou a má vontade do entrevistado;

e) decidir quanto à estrutura das questões;

f) determinar o fraseado das questões;

g) dispor as questões em ordem adequada;

h) identificar a forma e o *layout;*

i) reproduzir o questionário;

j) eliminar defeitos por meio de um pré-teste.

Assim sendo, entende-se que o questionário (Apêndice A) com perguntas fechadas de escolha única, enviado por correio eletrônico (*e-mail*), adaptou-se à proposta de pesquisa. Esse instrumento de coleta forneceu a possibilidade de alcançar com rapidez a amostra da população selecionada (concludentes e alunos do CEGSIC) que se encontra espalhada geograficamente, possibilitando, além disso, mais tempo e liberdade ao respondente, via de regra, fortemente engajado com os eventos de segurança de sua instituição.

3.4.3.2 Entrevista

Como instrumento de coleta complementar, caracterizando a pesquisa qualitativa, foi empregada a entrevista. Segundo Baptista e Cunha (2007, p.173), a entrevista focaliza a sua atenção nas causas das reações dos usuários da informação e na resolução do problema informacional, tendendo a aplicar um enfoque mais holístico, ao dar maior atenção aos aspectos subjetivos da experiência e do comportamento humano. Segundo Cunha (1982), a entrevista pode ser:

a) não estruturada: a iniciativa fica praticamente com o entrevistado, sendo bastante utilizada na pesquisa de mercado, psiquiatria e no serviço social;

b) semiestruturada: feita parcialmente com questões estruturadas, permitindo aprofundamento em tópicos julgados importantes pelo entrevistador;

c) estruturada: um esboço de perguntas ou formulário que é seguido pelo entrevistado.

Em conclusão, o autor esclarece as vantagens da entrevista:

a) possibilita o contacto direto com o entrevistado, tornando possível captar suas reações, sentimentos, hábitos etc.;

b) permite um maior grau de confiabilidade aos dados coletados;

c) por ser uma técnica face a face, possibilita que o entrevistador esclareça alguma pergunta ou terminologia não compreendida pelo entrevistado;

d) **o entrevistador pode pedir detalhes de respostas fornecidas quando são detectados fatos interessantes ou novos** [grifo nosso].

No caso, foi utilizada a entrevista focalizada ou semiestruturada, cujo roteiro de execução encontra-se no Apêndice B. Nesse tipo de entrevista é permitido ao entrevistado falar livremente sobre o assunto, cabendo ao entrevistador esforçar-se para manter o foco no tema original, particularmente, nas necessidades e usos da informação inerentes às atividades de segurança cibernética (GIL, 2008).

3.4.4 Análise dos dados

De acordo com Gil (2008, p. 156): "a análise tem como objetivo organizar e sumariar os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação". O autor observa os passos mais usuais da análise:

a) estabelecimento de categorias;

b) codificação;

c) tabulação;

d) análise estatística dos dados [caracterização do que é típico; distribuição dos indivíduos];

e) avaliação das generalizações obtidas pelos dados;

f) inferência das relações casuais;

g) interpretação dos dados.

Para tanto, foram aplicados elementos de estatística, de acordo com as considerações de Cervo, Bervian e Silva (2007): "outrora a estatística estava confinada à área das ciências exatas. [...] Atualmente, é considerada um dos mais úteis instrumentos de trabalho em todos os campos da investigação". Os autores, também, consideram, na fase de análise e interpretação, a grande valia da codificação dos dados em tabelas e gráficos, favorecendo a visualização do objeto da pesquisa por meio da representação material figurada. A concentração e simplificação do maior número de informações (multiplicação dos dados cifrados) no mesmo espaço, também, acabam facilitando as comparações, a análise e as interpretações.

No estudo em questão, foram relacionados os canais e fontes de informação levantados com as variáveis de relevância, acessibilidade e confiabilidade, bem como o mapeamento de possíveis usos da informação por meio das variáveis de frequência e pertinência.

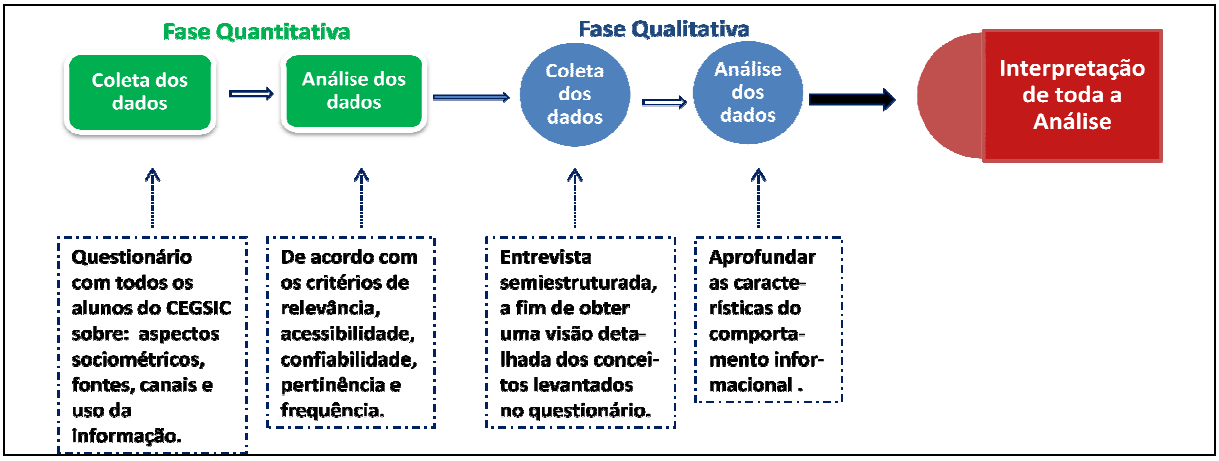
Foram estabelecidos diversos índices para as categorias (Índice B) e subcategorias (Índice A) de fontes e canais, bem como do uso da informação, a fim de correlacionar estatisticamente em relação às mesmas. No cálculo do Índice A foi utilizada média ponderada, enquanto no caso do Índice B foi utilizada média aritmética simples.

Em relação à análise dos dados das entrevistas, buscou-se um viés qualitativo, proporcionando, na opinião de Baptista e Cunha (2007), um enfoque mais holístico ao estudo, procurando captar a essência das experiências dos respondentes.

O exame do conteúdo extraído foi realizado com base na proposta de Laurence Bardin (2009). Para a pesquisadora, a análise de conteúdo, enquanto método, torna-se um conjunto de técnicas de análise das comunicações que utiliza procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens

Sintetizando os procedimentos metodológicos, a Figura 10 apresenta o modelo misto adotado (Explanatório) em conjunto com os instrumentos de coleta adotados.

Figura 10 - Procedimentos metodológicos da pesquisa



Fonte: elaboração própria

3.5 Relacionamento entre os Objetivos Específicos, Instrumentos de Coleta e Fontes da Pesquisa

A formalização da metodologia, de acordo com Lopez (2010), compreende, entre outros aspectos, a sistematização do que será feito para atingir cada um dos objetivos da pesquisa. Nesse sentido, o Quadro 9 relaciona os Objetivos Específicos (OE), as fontes e os procedimentos de coleta de dados, indicando, de maneira macro, os dados que se esperam coletar.

Quadro 9 - Relacionamento entre os OE e os dados da pesquisa

OBJETIVOS ESPECÍFICOS	MÉTODOS DE COLETA	FONTE	DADOS A SEREM COLETADOS
Identificar as fontes e os canais de informação mais utilizados pelos agentes públicos na gestão da segurança cibernética na APF	Revisão da literatura Questionário	Literatura especializada (Legislação da APF, Normas técnicas, livros e periódicos) CEGSIC	Fontes e canais de informação mais relevantes, acessíveis e confiáveis
Identificar os mais significativos usos da informação pelos agentes públicos, no contexto da segurança em um espaço cibernético numa organização da APF	Revisão da literatura Questionário Entrevista	Literatura especializada (livros, periódicos e anais de eventos) CEGSIC	Usos da informação mais frequentes e pertinentes
Mapear o comportamento informacional de um grupo representante de agentes públicos, quando envolvidos na segurança cibernética na APF	Questionário Entrevista	CEGSIC	Características do comportamento informacional

Fonte: elaboração própria

3.6 Estudo Piloto

3.6.1 Pesquisas realizadas

No segundo semestre de 2013, foi realizado um estudo piloto sobre as necessidades de informação dos profissionais de segurança do DATASUS\Ministério da Saúde.[36] O trabalho, entre outras finalidades, auxiliou no tocante à validação dos instrumentos utilizados na presente pesquisa. Dentre os aspectos mais relevantes, podem-se destacar os seguintes:

a) constatação de que os questionados identificaram e se autoenquadraram em perfis distintos, de acordo com as principais atividades desenvolvidas no contexto da segurança cibernética;

b) perguntas abertas identificaram outras formas de canais e fontes de informação, além das listadas nas questões fechadas;

c) importância da atualização e do acesso rápido às fontes.

A aprendizagem obtida com a pré-pesquisa norteou a reestruturação dos objetivos do trabalho, bem como a utilização de metodologia mista, envolvendo aspectos qualitativos além dos quantitativos.

No segundo semestre de 2014, foram analisados os procedimentos realizados pelos agentes responsáveis, quanto à gestão da segurança da Informação no espaço cibernético da APF, e buscou-se estabelecer os perfis que caracterizam os diferentes profissionais no trato dessa sensível área organizacional (WALLIER VIANNA; FERNANDES, 2014). O estudo fundamentou-se na análise dos Levantamentos de Governança de TI realizados pelo Tribunal de Contas da União, no período de 2007 a 2014, e nas informações coletadas durante a realização dos grandes eventos internacionais ocorridos no Brasil entre 2012 e 2014 (P.ex.: Rio + 20, Copa das Confederações 2013 e FIFA 2014).

Dessa forma, como um dos resultados alcançados no estudo supracitado, os procedimentos analisados foram agrupados sob três perspectivas de atuação (perfis) no contexto organizacional da segurança cibernética: nível operacional (atuação direta em sistemas computacionais, de controle ou rede de computadores), nível estratégico (coordenação, planejamento

[36] Maiores detalhes sobre a pesquisa consultar o artigo: Identificação das necessidades de informação dos profissionais de segurança da informação (MARQUES; WALLIER VIANNA, 2013).

e gestão de alto nível para alcançar resultados de longo prazo) e nível tático (ações de tratamento de incidentes de segurança em redes de computadores).[37]

3.6.2 Pré-teste

Fator crítico de sucesso na utilização do questionário é a aplicação de pré-testes. De acordo com Lakatos e Marconi (2010), depois de redigido, o questionário precisa ser testado antes de sua utilização definitiva, aplicando-se em uma pequena parcela da população escolhida, a fim de ser verificado se o mesmo possui validade (os dados colhidos são necessários à pesquisa) e operatividade (vocabulário acessível e significado claro). No presente estudo, o pré-teste do questionário foi aplicado, no período de 08 a 15 de julho de 2014, em dez servidores que trabalham com segurança cibernética em três organizações distintas da APF. Dessa forma, manteve-se coerência com as autoras supracitadas que afirmam: "o pré-teste [...] deve ser aplicado em populações com características semelhantes, mas nunca naquela que será alvo do estudo".

A aplicação do pré-teste possibilitou:

a) ajustes na apresentação das opções de resposta;

b) otimização na tabulação das respostas;

c) reformulação e acréscimo de questões;

d) retirada das questões abertas;

e) ratificação da necessidade da entrevista.

3.7 Coleta de Dados

As coletas de dados desse estudo dividiram-se em quantitativa e qualitativa.

3.7.1 Coleta Quantitativa

O questionário (Apêndice A), empregado na coleta de dados quantitativa, foi dividido em três blocos: (1) Identificação do perfil e do contexto das necessidades de informação, (2) Avaliação das principais fontes e canais de informação e, por último, (3) Uso da informação no desempenho das suas atividades no próprio ambiente de trabalho/Organização. Foi aplica-

[37] Artigo submetido/aceito pelo periódico Brazilian Journal of Information Science: research trends, aguardando publicação.

do nos alunos e ex-alunos do CEGSIC no período de 17 de outubro a 10 de novembro de 2014, sendo reenviado duas vezes com intervalos de sete dias.

Foram enviados 445 *e-mails* de acordo com a base de dados fornecida pela coordenação do curso, sendo que 8% mostraram-se inválidos, retornando com mensagem de erro (falha na entrega da mensagem). Cabe ressaltar que dos 412 *e-mails* válidos enviados, seria pertinente, ainda, desconsiderar os *e-mails* funcionais dos ex-alunos (turmas de 2008/2009 e 2010/2011) que mudaram de órgão, mas as caixas postais continuam disponíveis, aceitando *e-mails*. Não obstante, dos 412 questionários válidos enviados, 91 foram respondidos integralmente por alunos e ex-alunos, ou seja, 22 % da amostra real.

3.7.2 Coleta Qualitativa

De forma complementar, para a coleta qualitativa, foram entrevistados três servidores da APF no período de 3 a 5 de dezembro de 2014, a fim de aprofundar as características do comportamento informacional dos mesmos no contexto da pesquisa. Foram escolhidos agentes públicos de órgãos e áreas de atuação distintas, contemplando os três perfis de atuação no ambiente organizacional (estratégico, operacional e tático). O roteiro da Entrevista (Apêndice B) contempla os mesmos itens do questionário, com ênfase na validação do perfil em consonância com o uso da informação. Nesse caso, considerou-se que a informação é usada para responder a uma questão, solucionar uma situação-problema, negociar uma posição, sedimentar um ponto de vista ou tomar uma decisão.

Assim sendo, utilizou-se o princípio da saturação amostral que vem sendo aplicado em estudos sociais internacionais e nacionais. Dessa forma, em alguns estudos específicos (este incluso) não é necessária uma grande quantidade de entrevistas, mas sim uma qualidade de entrevistas dirigidas, abrangendo pessoas certas e pretendidas.

No capítulo seguinte, são apresentados e analisados os resultados da pesquisa, organizados nas seguintes categorias: (1) Perfil e Necessidades de Informação, (2) Fontes e Canais de Informação e (3) Usos da Informação.

4 ANÁLISE

Em consonância com a estratégia de investigação da presente pesquisa, qual seja a utilização do modelo misto Explanatório, detalhado pela Figura 10: Procedimentos metodológicos da pesquisa, a análise dos dados compreende duas fases: a primeira corresponde aos dados coletados por meio da aplicação do questionário (amostragem quantitativa), enquanto que a segunda fase refere-se às entrevistas realizadas (qualitativa).

Na primeira fase, a análise estatística dos dados obtidos por meio do questionário foi feita, basicamente, mediante a tabulação dos 91 *e-mails* recebidos que propiciaram a criação de gráficos e de tabelas. A coleta dos dados dos questionários respondidos foi realizada por meio do aplicativo de pesquisa Google Docs[38] e possibilitou inferir os resultados obtidos na amostra (alunos do CEGSIC) para a população da qual foi extraída (agentes públicos responsáveis pela gestão da segurança cibernética na APF).

A fim de identificar o perfil da amostra e contextualizar as necessidades de informação, foi questionado: Sexo, Idade, Tempo de Experiência na Área, Tempo de Trabalho na Organização, Formação Acadêmica, Formação ou Capacitação mais utilizada no trabalho, bem como Tarefas Primárias e Secundárias realizadas de acordo com os perfis pré-estabelecidos (estratégico, operacional e tático). Para descrição do comportamento de busca, a estratégia utilizada foi a de levantar informações sobre as principais fontes e canais de informação utilizados, com base nas variáveis: relevância, confiabilidade e acessibilidade.

No caso da identificação dos usos de informação, buscou-se mapear os procedimentos mais usuais inerentes aos perfis pré-estabelecidos, sendo que as variáveis escolhidas foram frequência e pertinência. As cinco variáveis estabelecidas são entendidas, neste estudo, da seguinte forma:

a) relevância: a informação possui um elevado grau de utilidade para o alcance de um objetivo, subsidiando um processo de decisão;
b) confiabilidade: percepção de idoneidade e de credibilidade no conteúdo de uma fonte ou canal de informação;
c) acessibilidade: facilidade e disponibilidade de acesso às fontes e canais de informação;
d) frequência: quantidade de vezes em que um determinado tipo de informação é acessado por uma unidade de tempo;

[38] Disponível em <http://docs.Google.com>. Acesso em: 02 mar. 2014.

e) pertinência: o tipo de informação é apropriado e importante às atividades realizadas.

A tabulação foi realizada com o auxílio do *software* Microsoft Excel®, no qual foram efetuados os cálculos necessários à obtenção dos resultados para análise, para a elaboração de tabelas, bem como para a produção de gráficos.

A utilização de Gráfico de Setores na tabulação e na análise dos dados do 1º Bloco do questionário - identificação do perfil e do contexto das necessidades de informação - possibilitou mostrar diferenças de valores percentuais em relação ao total dos questionados.

Na tabulação dos dados do 2º Bloco - avaliação dos principais canais e fontes de informação - foram calculados e concentrados matricialmente em tabelas:

a) os valores percentuais das respostas dos participantes escalonados em cinco colunas, sendo a primeira referente a não utilização da fonte e as demais abordando a variável questionada em escala crescente;

b) os valores dos índices para cada Categoria (Índice B), aferidos por meio da média aritmética simples do Índice A (das subcategorias afins);

c) os valores dos índices para cada Subcategoria (Índice A), aferidos por meio da média ponderada dos valores percentuais das cinco respostas possíveis para cada variável questionada. No cálculo do Índice A foi utilizado pesos crescentes de 1 (menos) a 4 (mais) e 0 para fonte não utilizada .

Na tabulação dos dados do 3º Bloco - uso da informação no desempenho das suas atividades no seu ambiente de trabalho/Organização -, de igual forma, foram calculados e concentrados matricialmente em tabelas: os valores percentuais das respostas dos participantes sobre o uso da informação, bem como os valores dos índices para cada Subcategoria (Índice A) aferidos de maneira idêntica ao 2º Bloco.

As fontes/canais e os usos da informação permaneceram ordenados de acordo com a sequência do questionário, sendo ressaltados em cinza, os valores máximos e mínimos em cada uma das cinco variáveis estabelecidas.

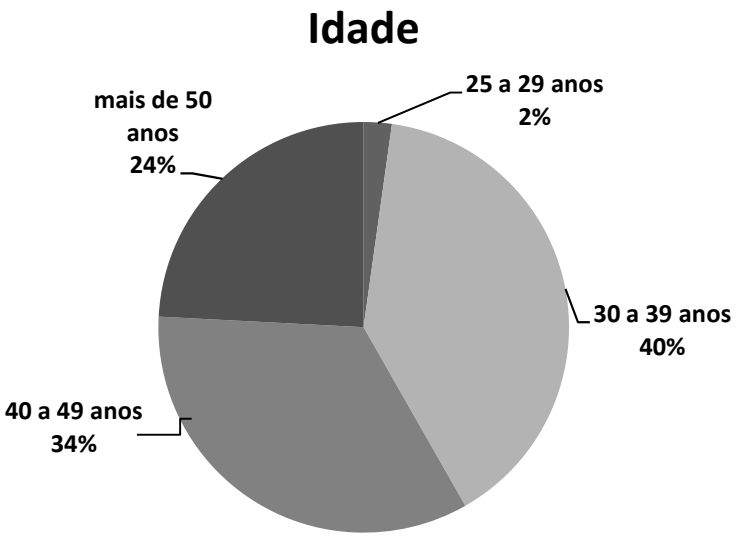
Na segunda fase da análise, as informações mais esclarecedoras e pertinentes extraídas das entrevistas, realizadas pelo próprio pesquisador, foram inseridas ao longo da 1ª fase da análise. No caso, foi utilizado pelo pesquisador o método de condensação dos significados, no qual aquilo que é dito pelo entrevistado é resumido em formulações mais breves e sucintas. Depois de sintetizadas e consolidadas, as respostas foram agrupadas, a fim de compor um todo que possibilitasse um relacionamento entre elas.

4.1 Perfil e Necessidades de Informação

Nessa primeira parte do questionário, verificou-se que a amostra é pouco diversificada em termos de sexo, com 86% de homens; ratificando o encontrado em trabalhos relacionados às necessidades informacionais no ambiente cibernético tais como: Ohtoshi (2013) e Mafra Pereira e Barbosa (2008). Dentro da expectativa do autor, além da predominância masculina, 58% dos pesquisados possuem 40 anos ou mais, demonstrando a importância do amadurecimento etário daqueles que trabalham em segurança cibernética, como apresentado no Gráfico 1.

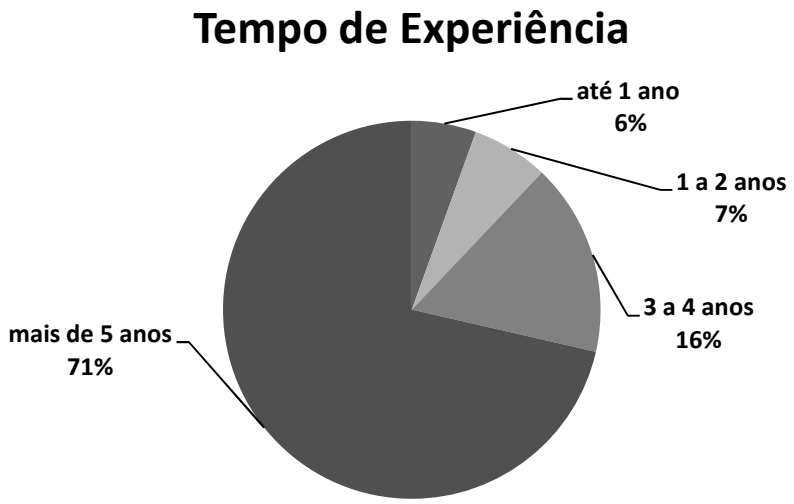
Nessa linha, e de acordo com o Gráfico 2, corrobora-se o fato de que o tempo de experiência na área também é elevado, com aproximadamente três quartos dos respondentes com mais de cinco anos de experiência.

Gráfico 1 - Distribuição da Idade



Fonte: elaboração própria

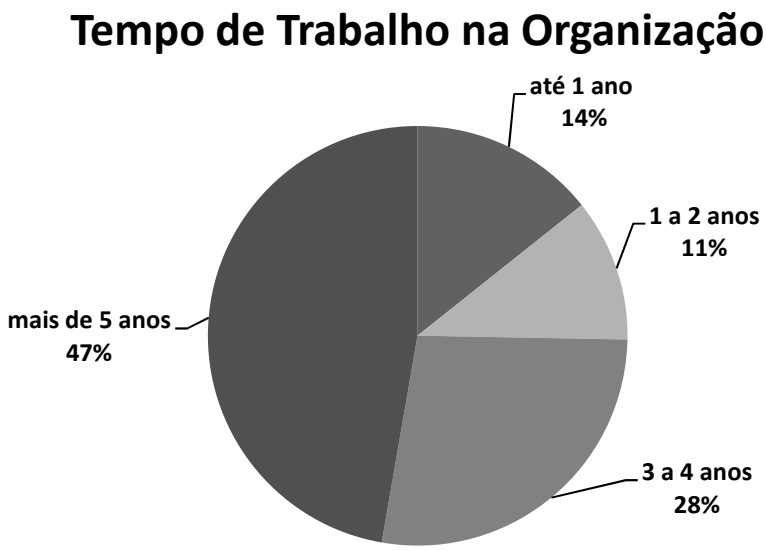
Gráfico 2 - Tempo de Experiência na Área



Fonte: elaboração própria

Apesar de um pouco mais diversificado, no Gráfico 3, constatou-se que quase metade dos questionados permaneceram nas mesmas organizações há mais de cinco anos. Tal fato não deixa de ser surpreendente por motivos diversos como: promoções na carreira, realização de novos concursos públicos e busca de melhores de salários na iniciativa privada, que podem elevar a rotatividade dos profissionais que lidam com segurança no âmbito da APF.

Gráfico 3 - Tempo de Trabalho na Organização

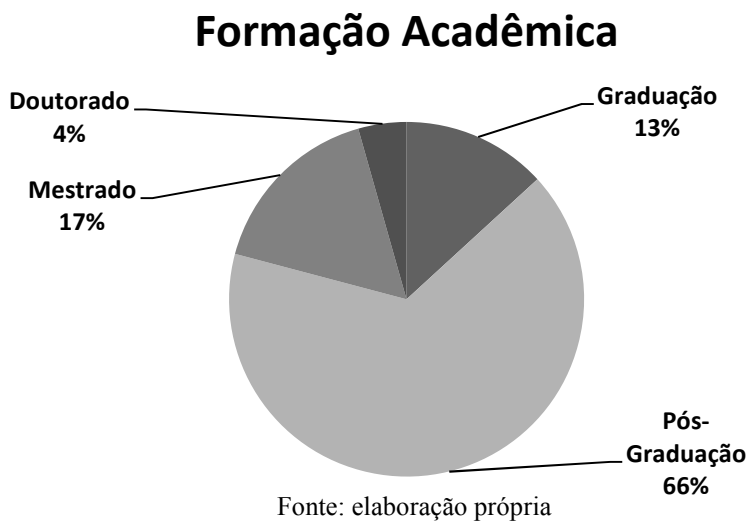


Fonte: elaboração própria

Em termos de Formação Acadêmica, ressalta-se, no Gráfico 4, o reduzido índice de pós- graduação s*tricto sensu*, onde apenas um quinto dos respondentes possuem mestrado ou doutorado. O fato torna-se ainda mais intrigante, quando se leva em consideração a faixa etária madura e a elevada experiência na área.

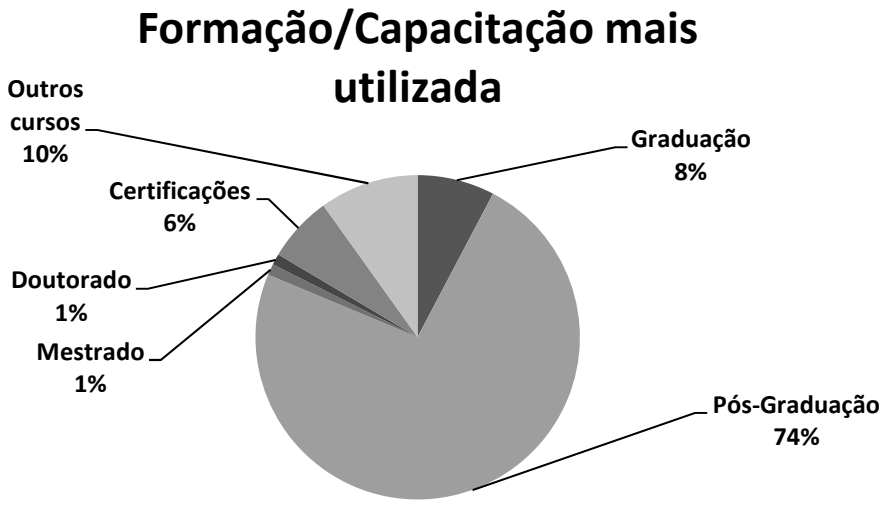
Nesse contexto, quando se trata de Capacitação mais utilizada no desempenho das atividades no ambiente de trabalho (Gráfico 5), percebe-se a importância esmagadora da pós-graduação *lato sensu* em detrimento da *stricto sensu* (74% contra 2%), bem como a sugestiva utilização de Certificações e cursos técnicos (16%) de curta duração na lide diária.

Gráfico 4 - Formação Acadêmica



Fonte: elaboração própria

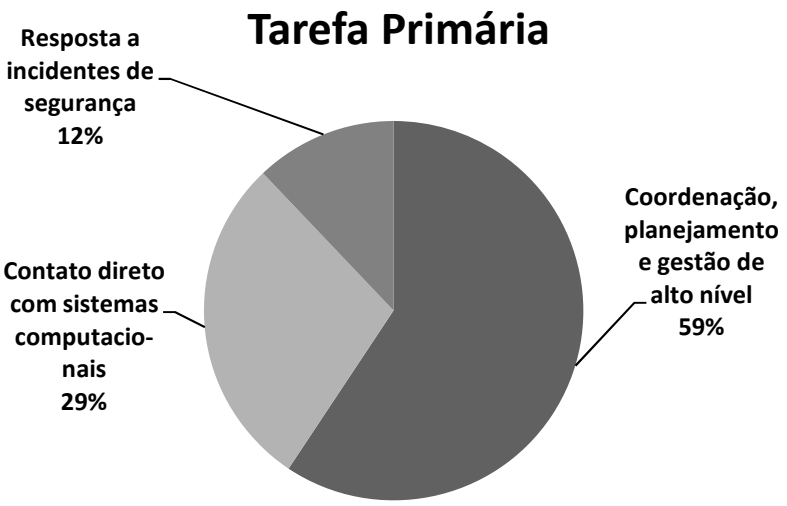
Gráfico 5 - Formação/Capacitação mais utilizada



Fonte: elaboração própria

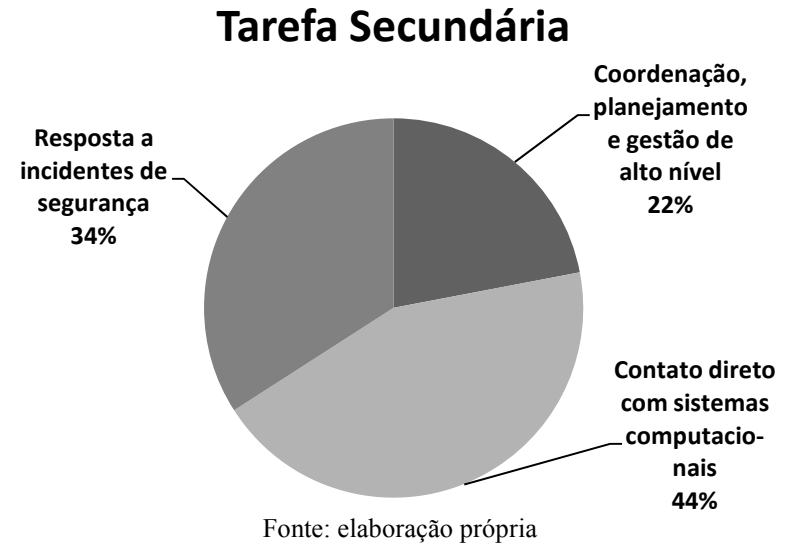
Os gráficos 6 e 7 seguintes representam, respectivamente, as Tarefas Primárias (TP) e Secundárias (TS) realizadas pelos respondentes. Fazendo o cruzamento entre os gráficos, fica evidente que a maioria divide-se entre atividades de cunho estratégico (59% - TP & 22% - TS) e operacional (29% - TP & 44% - TS).

Gráfico 6 - Tarefa Primária realizada



Fonte: elaboração própria

Gráfico 7 - Tarefa Secundária realizada



Fonte: elaboração própria

Os agentes públicos responsáveis pela gestão da segurança da informação no espaço cibernético na APF ocupam-se, prioritariamente, dos cuidados necessários com a segurança da informação institucional, na sua expressão mais abrangente, incluindo pessoas, processos e tecnologia, bem como ações corporativas de segurança cibernética. Em segundo lugar, dedi-

cam-se às atividades técnicas que asseguram o correto funcionamento dos recursos de TIC da Organização, conforme ilustrado no relato abaixo:

> Após um tempo na área operacional, estou voltando para ações de gestão, como atualização das normas e realização de atividades de contratação de material e de serviços de TIC, com base nas normas do Ministério do Planejamento. (Entrevista 1)

4.2 Fontes e Canais de Informação

Em relação ao relacionamento do potencial usuário, com as fontes e canais de informação, foram utilizadas duas classes: **Pessoais** (informais) onde as informações são transmitidas diretamente, pessoa a pessoa, através de contatos interpessoais e **Impessoais** (formais) onde as informações são registradas e disseminadas de forma impressa ou digitalizada, através de fontes primárias e secundárias. No que se referem à sua origem, as fontes de informação foram segmentadas em **Externas** ou **Internas** à organização do usuário.

Dessa forma, foram compostas quatro categorias: Pessoal Externa (PE), Pessoal Interna (PI), Impessoal Externa (IE) e Impessoal Interna (II), as quais foram selecionadas durante a realização da Revisão da Literatura (Seção 2.4). Cabe ressaltar que não foi efetuada distinção entre fontes/canais eletrônicos e não eletrônicos como sugerem Mafra Pereira e Barbosa (2008). Tal decisão originou-se da elevada interação, por parte dos alunos do CEGSIC, entre pessoa-computador-pessoa, que é possibilitada pelo uso intensivo da rede mundial de computadores - Internet. Essas quatro categorias foram divididas em subcategorias conforme o Quadro 10.

Quadro 10 - Fontes e Canais de informação na Segurança Cibernética

Categorias	**Pessoal**	**Impessoal**
Externa	Encontros oficiais (seminários, congressos etc.) Conversa com fornecedores, consultores e outros Mídias sociais (fóruns, *chats*, listas, *blogs* etc.) Conversa com ex-colegas de cursos	Publicações governamentais (normas, manuais) Livros impressos ou eletrônicos Revistas e artigos científicos Anais de congressos científicos Trabalhos/resumos de áreas afins Mecanismos de busca na Internet Portais de empresas, organizações de segurança
Interna	Encontros oficiais (debates, palestras etc.) Conversa com colegas Conversa com chefes/supervisores Reuniões informais	Mídias sociais (fóruns, *chats*, listas, *blogs* etc.) Base de dados (sistemas, relatórios, políticas)

Fonte: Adaptado de Choo (1994)

As dezessete subcategorias foram objeto de questionamento nas três variáveis consideradas: relevância, confiabilidade, acessibilidade, as quais se encontram organizadas matricialmente nas tabelas a seguir.

4.2.1 Relevância

Tabela 1 - Avaliação percentual da Relevância por categorias e subcategorias

CATEGORIAS	SUBCATEGORIAS	não utiliza a fonte (%)	Irrelevante (%)	Pouco Relevante (%)	Relevante (%)	Muito Relevante (%)	Índice A - SUB-CATEGORIA (1)	Índice B CA-TEGORIA (1)
PESSOAL EXTERNA À ORGANIZAÇÃO	B1 Encontros oficiais (seminários, congressos etc.)	3,3	1,1	11,0	38,5	46,2	3,23	3,04
	B2 Conversa com fornecedores, consultores e outros	5,5	3,3	19,8	38,5	33,0	2,90	
	B3 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	7,7	2,2	23,1	41,8	25,3	2,75	
	B4 Conversa com ex-colegas de cursos	4,4	3,3	6,6	33,0	52,7	3,26	
PESSOAL INTERNA À ORGANIZAÇÃO	B5 Encontros oficiais (debates, palestras etc.)	4,4	5,5	15,4	26,4	48,4	3,09	3,16
	B6 Conversa com colegas	1,1	4,4	4,4	30,8	59,3	3,43	
	B7 Conversa com chefes/supervisores	3,3	4,4	11,0	25,3	56,0	3,26	
	B8 Reuniões informais	4,4	6,6	15,4	45,1	28,6	2,87	
IMPESSOAL EXTERNA À ORGANIZAÇÃO	B11 Publicações governamentais (normas, manuais)	0,0	1,1	6,6	34,1	58,2	3,49	3,16
	B12 Livros impressos ou eletrônicos	5,5	2,2	6,6	34,1	51,6	3,24	
	B13 Revistas e artigos científicos	4,4	2,2	8,8	28,6	56,0	3,30	
	B14 Anais de congressos científicos	9,9	3,3	8,8	35,2	42,9	2,98	
	B15 Trabalhos/resumos de áreas afins	4,4	3,3	13,2	42,9	36,3	3,03	
	B16 Mecanismos de busca na internet (google, cade)	0,0	5,5	19,8	36,3	38,5	3,08	
	B17 Portais de empresas, organizações de segurança	2,2	0,0	22,0	46,2	29,7	3,01	

IMPESSOAL INTERNA À ORGANIZAÇÃO	B9 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	11,0	5,5	29,7	23,1	30,8	2,57	2,93
	B10 Base de dados (sistemas, relatórios, políticas)	1,1	5,5	8,8	31,9	52,7	3,30	

Fonte: elaboração própria

[a] No cálculo do Índice A (média ponderada) foram estabelecidos os seguintes pesos: 0 para Não utiliza a fonte; 1 para Irrelevante; 2 para Pouco Relevante; 3 para Relevante e 4 para Muito Relevante.

[b] Média aritmética simples.

Verifica-se, a partir da análise da Tabela 1, que os pesquisados consideram de maior relevância as categorias Pessoal Interna e Impessoal Externa à organização, as quais apresentaram o mesmo índice 3,16 (Índice B) de relevância. Em relação ao Índice A, referente às subcategorias de fontes de informação, destaca-se a relevância elevada para as conversas com colegas, chefes/supervisores e para as publicações governamentais. Soma-se aos fatos acima o relato de um dos entrevistados:

> A pesquisa geral sobre segurança está na Internet e na Intranet dos órgãos da APF, mas tem que ser feita uma filtragem, uma análise nessas bases de dados. Além das pessoas, no bate-papo do cafezinho, com servidores que trabalham ou já trabalharam com os assuntos pesquisados. (Entrevista 1)

Destaca-se, também, a baixa relevância atribuída às mídias sociais (fóruns, *chats*, listas, *blogs* etc.) internas à organização com o menor Índice A (2,57) da Tabela 1. Acredita-se que tal fato deve-se à baixa utilização, aliada, provavelmente, à ineficácia, ou mesmo à inexistência de tal serviço. Ainda no quesito da relevância, nota-se que todos os respondentes não dispensam consultar as publicações governamentais (normas, manuais), bem como os mecanismos de busca na Internet (Google, Bing).

4.2.2 Confiabilidade

Tabela 2 - Avaliação percentual da Confiabilidade por categorias e subcategorias

CATEGORIAS	**SUBCATEGORIAS**	**Não utiliza a fonte (%)**	**Nem um pouco Confiável (%)**	**Pouco Confiável (%)**	**Confiável (%)**	**Muito Confiável (%)**	**Índice A - SUBCATEGORIA [1]**	**Índice B CATEGORIA [1]**
PESSOAL EXTERNA À ORGANIZAÇÃO	B1 Encontros oficiais (seminários, congressos etc.)	3,3	2,2	22,0	46,2	26,4	2,90	2,55
	B2 Conversa com fornecedores, consultores e outros	5,5	14,3	31,9	38,5	9,9	2,33	
	B3 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	8,8	16,5	41,8	28,6	4,4	2,03	
	B4 Conversa com ex-colegas de cursos	4,4	3,3	12,1	52,7	27,5	2,96	

PESSOAL INTERNA À ORGANIZAÇÃO	B5 Encontros oficiais (debates, palestras etc.)	4,4	6,6	18,7	31,9	38,5	2,93	2,93
	B6 Conversa com colegas	1,1	3,3	12,1	42,9	40,7	3,19	
	B7 Conversa com chefes/supervisores	2,2	6,6	15,4	42,9	33,0	2,98	
	B8 Reuniões informais	5,5	8,8	19,8	48,4	17,6	2,64	
IMPESSOAL EXTERNA À ORGANIZAÇÃO	B11 Publicações governamentais (normas, manuais)	2,2	2,2	8,8	31,9	54,9	3,35	2,85
	B12 Livros impressos ou eletrônicos	5,5	4,4	11,0	42,9	36,3	3,00	
	B13 Revistas e artigos científicos	4,4	2,2	12,1	42,9	38,5	3,09	
	B14 Anais de congressos científicos	8,8	1,1	9,9	42,9	37,4	2,99	
	B15 Trabalhos/resumos de áreas afins	4,4	4,4	22,0	46,2	23,1	2,79	
	B16 Mecanismos de busca na internet (google, cade)	3,3	15,4	42,9	29,7	8,8	2,25	
	B17 Portais de empresas, organizações de segurança	2,2	9,9	35,2	40,7	12,1	2,51	
IMPESSOAL INTERNA À ORGANIZAÇÃO	B9 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	12,1	14,3	23,1	33,0	17,6	2,30	2,74
	B10 Base de dados (sistemas, relatórios, políticas)	0,0	7,7	12,1	34,1	46,2	3,19	

Fonte: elaboração própria

[a] No cálculo do Índice A (Média Ponderada) foram estabelecidos os seguintes pesos: 0 para Não utiliza a fonte; 1 para Nem um Pouco Confiável; 2 para Pouco Confiável; 3 para Confiável e 4 para Muito Confiável.

[b] Média aritmética simples.

Do ponto de vista da confiabilidade, na Tabela 2 percebe-se, também, a preferência pelas fontes/canais intrínsecos à organização e de relacionamento pessoal, cujo valor obtido (Índice B) foi de 2,93, com destaque para as subcategorias: Conversa com colegas do trabalho e Conversa com chefes/supervisores. Entretanto, a maior confiabilidade foi atribuída à subcategoria Publicações Governamentais, da categoria Impessoal Externa, que apresentou índice de 3,35.

Também em relevo, observa-se, na subcategoria Base de dados (sistemas, relatórios, políticas) interna à Organização, o elevado Índice de 3,19 para confiabilidade e a plena utilização por parte dos respondentes. Ainda no quesito confiabilidade, ressalta-se que mais de 60% dos questionados não confiam nos mecanismos de Busca na Internet. Não obstante, um dos entrevistados destacou:

> Em relação à confiabilidade, busco, na Internet, artigos e orientações de empresas internacionais de soluções de segurança cibernética como antivírus etc., para auxiliar na solução de novos dos problemas. (Entrevista 2)
>
> Também são buscadas informações em comunidades que desenvolvem ou trabalham com sistemas operacionais e banco de dados semelhantes. (Entrevista 3)

4.2.3 Acessibilidade

Tabela 3 - Avaliação percentual da Acessibilidade por categorias e subcategorias

CATEGORIAS	SUBCATEGORIAS	Não utiliza a fonte (%)	Muito Difícil o Acesso %	Difícil Acesso %	Acessível (%)	Fácil Acesso (%)	Índice A - SUBCATE-GORIA (a)	Índice B CA-TEGORIA (b)
PESSOAL EXTERNA À ORGANIZAÇÃO	B1 Encontros oficiais (seminários, congressos etc.)	4,4	11,0	29,7	37,4	17,6	2,53	2,63
	B2 Conversa com fornecedores, consultores e outros	6,6	8,8	25,3	39,6	19,8	2,57	
	B3 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	8,8	5,5	19,8	37,4	28,6	2,71	
	B4 Conversa com ex-colegas de cursos	5,5	9,9	18,7	41,8	24,2	2,69	
PESSOAL INTERNA À ORGANIZAÇÃO	B5 Encontros oficiais (debates, palestras etc.)	5,5	9,9	28,6	30,8	25,3	2,60	2,77
	B6 Conversa com colegas	4,4	5,5	13,2	31,9	45,1	3,08	
	B7 Conversa com chefes/supervisores	5,5	13,2	18,7	34,1	28,6	2,67	
	B8 Reuniões informais	6,6	6,6	18,7	45,1	23,1	2,71	
IMPESSOAL EXTERNA À ORGANIZAÇÃO	B11 Publicações governamentais (normas, manuais)	1,1	4,4	15,4	26,4	52,7	3,25	2,71
	B12 Livros impressos ou eletrônicos	5,5	9,9	17,6	40,7	26,4	2,73	
	B13 Revistas e artigos científicos	7,7	6,6	29,7	31,9	24,2	2,58	
	B14 Anais de congressos científicos	16,5	13,2	26,4	29,7	14,3	2,12	
	B15 Trabalhos/resumos de áreas afins	6,6	17,6	33,0	31,9	11,0	2,23	
	B16 Mecanismos de busca na Internet (Google, Bing)	0,0	3,3	14,3	27,5	54,9	3,34	
	B17 Portais de empresas, organizações de segurança	3,3	8,8	18,7	48,4	20,9	2,75	

IMPESSOAL INTERNA À ORGANIZAÇÃO	B9 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	13,2	13,2	26,4	24,2	23,1	2,31	2,56
	B10 Base de dados (sistemas, relatórios, políticas)	4,4	6,6	23,1	35,2	30,8	2,81	

Fonte: elaboração própria

[a] No cálculo do Índice A (Média Ponderada) foram estabelecidos os seguintes pesos: 0 para Não utiliza a fonte; 1 para Muito Difícil o Acesso; 2 para Difícil Acesso; 3 para Accessível e 4 para Fácil Acesso.

[b] Média aritmética simples.

De acordo com a Tabela 3, mostraram-se mais acessíveis às fontes e canais oriundos da categoria Pessoal Interna (Índice B=2,77), enquanto que uma menor acessibilidade foi percebida na categoria Impessoal Interna à Organização (Índice B=2,56). Na contramão desse índice, mesmo que de forma não científica, de acordo com o relato abaixo, percebe-se a importância dessa categoria:

> O conjunto dos livros e do material dos cursos, somados a documentos de elaboração interna própria (procedimentos padronizados) e dos demais colegas do ambiente de trabalho, forma uma espécie de biblioteca particular e técnica da equipe. (Entrevista 2)

Não obstante, o maior destaque coube à categoria Impessoal Externa à Organização, onde as subcategorias Publicações governamentais e Mecanismos de busca na Internet obtiveram os maiores índices com 3,25 e 3,34, respectivamente. Destaca-se, ainda, que todos os questionados utilizam os Mecanismos de busca na Internet.

Observa-se, também, que a maioria dos respondentes possui dificuldade de acesso (Difícil, Muito Difícil e Não utiliza) às seguintes subcategorias Impessoais de informação: Mídias sociais internas à Organização (52,8%), Anais de congressos científicos (56,1%) e Trabalhos/resumos de áreas afins (56,2%).

4.2.4 Relacionamento entre relevância, confiabilidade e acessibilidade

A Tabela 4 resume a análise por relevância, confiabilidade e acessibilidade, ordenando as principais fontes/canais de informação por essas três variáveis. A referida tabela foi organizada a partir do Índice A e pode-se percebe que três subcategorias destacam-se das demais: Publicações governamentais, Conversa com colegas de trabalho e Base de dados interna à Organização.

Tabela 4 - Resumo da análise por Relevância, Confiabilidade e Acessibilidade

VARIÁVEL	TIPOS DE FONTES	SUBCATEGORIAS
RELEVÂNCIA	Impessoal Externa	Publicações governamentais (normas, manuais)
	Pessoal Interna	Conversa com colegas
	Impessoal Externa	Revistas e artigos científicos
	Impessoal Interna	Base de dados (sistemas, relatórios, políticas)
CONFIABILIDADE	Impessoal Externa	Publicações governamentais (normas, manuais)
	Impessoal Interna	Base de dados (sistemas, relatórios, políticas)
	Pessoal Interna	Conversa com colegas
	Impessoal Externa	Revistas e artigos científicos
ACESSIBILIDADE	Impessoal Externa	Mecanismos de busca na Internet (Google, Bing)
	Impessoal Externa	Publicações governamentais (normas, manuais)
	Pessoal Interna	Conversa com colegas
	Impessoal Interna	Base de dados (sistemas, relatórios, políticas)

Fonte: elaboração própria

Para a análise entre as variáveis empregadas no comportamento de busca da informação, foram elaboradas as Tabelas 5 e 6 que relacionam a relevância das fontes e canais de informação com a confiabilidade e a acessibilidade, respectivamente.

Em relação às categorias e subcategorias, levou-se em consideração a variação entre os respectivos índices. No caso, considera-se que, quanto menor a variação entre eles, maior será a racionalidade na utilização das fontes/canais de informação. As variações mais elevadas, ou mesmo as negativas, foram destacadas (cinza) e podem indicar quais fontes de informação merecem atenção especial, a fim de se reduzirem os descompassos evidenciados.

A Tabela 5, a seguir, demonstra que, apesar de pouco confiáveis, as fontes externas como as Mídias sociais e os Mecanismos de busca na Internet são consideradas relevantes para os agentes públicos. De fato, a maior variação entre relevância e confiabilidade foi registrada na categoria Pessoal Externa, com índice de 0,48.

Tabela 5 - Relacionamento entre Relevância e Confiabilidade

CATEGORIAS	SUBCATEGORIAS	Índice A - RELEVÂNCIA	Índice A - CONFIABILIDADE	Variação Índice A - RELEVÂNCIA e CONFIABILIDADE	Índice B - RELEVÂNCIA	Índice B - CONFIABILIDADE	Variação Índice B - RELEVÂNCIA e CONFIABILIDADE
PESSOAL EXTERNA À ORGANIZAÇÃO	B1 Encontros oficiais (seminários, congressos etc.)	3,23	2,90	0,33	3,04	2,55	0,48
	B2 Conversa com fornecedores, consultores e outros	2,90	2,33	0,57			
	B3 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	2,75	2,03	0,71			
	B4 Conversa com ex-colegas de cursos	3,26	2,96	0,31			
PESSOAL INTERNA À ORGANIZAÇÃO	B5 Encontros oficiais (debates, palestras etc.)	3,09	2,93	0,15	3,16	2,93	0,23
	B6 Conversa com colegas	3,43	3,19	0,24			
	B7 Conversa com chefes/supervisores	3,26	2,98	0,29			
	B8 Reuniões informais	2,87	2,64	0,23			
IMPESSOAL EXTERNA À ORGANIZAÇÃO	B11 Publicações governamentais (normas, manuais)	3,49	3,35	0,14	3,16	2,85	0,31
	B12 Livros impressos ou eletrônicos	3,24	3,00	0,24			
	B13 Revistas e artigos científicos	3,30	3,09	0,21			
	B14 Anais de congressos científicos	2,98	2,99	-0,01			
	B15 Trabalhos/resumos de áreas afins	3,03	2,79	0,24			
	B16 Mecanismos de busca na Internet (Google, Bing)	3,08	2,25	0,82			
	B17 Portais de empresas, organizações de segurança	3,01	2,51	0,51			
IMPESSOAL INTERNA À ORGANIZAÇÃO	B9 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	2,57	2,30	0,27	2,93	2,74	0,19
	B10 Base de dados (sistemas, relatórios, políticas)	3,30	3,19	0,11			

Fonte: elaboração própria

Especialmente no caso dos Mecanismos de busca, a Tabela 6 apresenta discreta variação negativa, ou seja, a facilidade de acesso (e o próprio acesso como foi confirmado nas entrevistas) é desproporcionalmente superior à própria relevância dessa fonte.

Tabela 6 - Relacionamento entre Relevância e Acessibilidade

CATEGORIAS	SUBCATEGORIAS	Índice A - RELEVÂNCIA	Índice A - ACESSIBILIDADE	Variação Índice A - RELEVÂNCIA e ACESSIBILIDADE	Índice B - RELEVÂNCIA	Índice B - ACESSIBILIDADE	Variação Índice B - RELEVÂNCIA e ACESSIBILIDADE
PESSOAL EXTERNA À ORGANIZAÇÃO	B1 Encontros oficiais (seminários, congressos etc.)	3,23	2,53	0,70	3,04	2,63	0,41
	B2 Conversa com fonecedores, consultores e outros	2,90	2,57	0,33			
	B3 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	2,75	2,71	0,03			
	B4 Conversa com ex-colegas de cursos	3,26	2,69	0,57			
PESSOAL INTERNA À ORGANIZAÇÃO	B5 Encontros oficiais (debates, palestras etc.)	3,09	2,60	0,48	3,16	2,77	0,39
	B6 Conversa com colegas	3,43	3,08	0,35			
	B7 Conversa com chefes/supervisores	3,26	2,67	0,59			
	B8 Reuniões informais	2,87	2,71	0,15			
IMPESSOAL EXTERNA À ORGANIZAÇÃO	B11 Publicações governamentais (normas, manuais)	3,49	3,25	0,24	3,16	2,71	0,45
	B12 Livros impressos ou eletrônicos	3,24	2,73	0,52			
	B13 Revistas e artigos científicos	3,30	2,58	0,71			
	B14 Anais de congressos científicos	2,98	2,12	0,86			
	B15 Trabalhos/resumos de áreas afins	3,03	2,23	0,80			
	B16 Mecanismos de busca na Internet (Google, Bing)	3,08	3,34	-0,26			
	B17 Portais de empresas, organizações de segurança	3,01	2,75	0,26			
IMPESSOAL INTERNA À ORGANIZAÇÃO	B9 Mídias sociais (fóruns, *chats*, listas, *blogs* etc.)	2,57	2,31	0,26	2,93	2,56	0,37
	B10 Base de dados (sistemas, relatórios, políticas)	3,30	2,81	0,48			

Fonte: elaboração própria

Aspectos referentes à diversidade de fontes e à importância dos cruzamentos das variáveis, mesmo em ambiente organizacional, podem ser observados no relato a seguir:

> A gente também trabalha com sistemas de Wiki [Wikipédia ou enciclopédia virtual]. Todos os nossos procedimentos são documentados, tanto a parte de instalação de equipamentos como a de serviços são documentados no Wiki interno e isso serve para consultas futuras. Mas, para construir esse conhecimento, a gente busca na Internet e tem que saber filtrar na Internet as informações que vão nos ajudar. Depois de testar as informações obtidas em laboratório e customizá-las aos requisitos de segurança da organização, é que as mesmas são adicionadas ao nosso Wiki. (Entrevista 3)

Cabe destacar que essa fonte de informação interna e impessoal não é formalizada pela instituição, ou seja, ela é administrada e atualizada pelos próprios integrantes do setor onde o entrevistado trabalha, de maneira empírica, sem a supervisão de um profissional de Informação.

4.3 Usos da Informação

Conforme descrito ao longo da pesquisa, sugere-se que os papéis desempenhados pelos agentes públicos, que atuam na segurança do espaço cibernético da APF, sejam caracterizados em três perfis: estratégico, operacional e tático. Tais perfis ou níveis de atuação proporcionam, diuturnamente, diversas situações-problema que devem ser enfrentadas com tempestividade. Ao lidarem com essas situações, é possível que experimentem o processo de "necessidade informacional", ou seja, que reconheçam a sua eventual incapacidade de solucionar o referido problema técnico com base nas informações de que já dispõem. O relato a seguir ratificou esse entendimento:

> O que gera a necessidade de busca da informação é quando chega um incidente de rede diferente, uma situação que foge ao nosso conhecimento [...] é buscado em várias fontes. Pode ser na Internet como os mecanismos de busca principais, uso muito o Google, as enciclopédias livres, tipo Wikipedia e uma pilha de livros pessoais técnicos e de material de cursos do Cert.br. Além, é claro, das pessoas que compõem a equipe de trabalho. (Entrevista 2)

Dessa forma, sete "usos" rotineiros da informação (perguntas C1 a C7), inerentes aos três níveis pré-estabelecidos, foram avaliados sob as variáveis de frequência e pertinência. As tabelas 7 e 8 concentram as respostas referentes à não utilização da informação ou à sua utilização em quatro períodos temporais: ano, mês, semana e dia.

4.3.1 Frequência

Como esperado pelo autor, e de acordo com a Tabela 7, o maior uso da informação foi registrado nas atividades de aprimoramento da segurança da informação no espaço cibernético inerente à organização com índice de 2,60 e uso diário por mais de um quarto dos respondentes. O uso da informação para atividades de Aprendizado, ou seja, para a aquisição de novos conhecimentos que poderão utilizados ser na solução de problemas futuros, também se destaca positivamente (índice de 2,51), aparecendo como segundo tipo de uso mais frequente da informação na pesquisa realizada, corroborando com o apurado por Ohtoshi (2013).

Não obstante, surpreendeu constatar-se o baixo uso das informações para atividades de auditoria em sistemas computacionais comprometidos, onde, praticamente, um quarto dos respondentes nem sequer utilizam fontes sobre o tema.

Tabela 7 - Avaliação percentual da Frequência por uso da informação

USO DA INFORMAÇÃO	Não utiliza (%)	1 vez ao ano %	1 vez ao mês %	1 vez na semana (%)	1 vez ao dia (%)	Índice A - SUBCATEGORIA ([a])
C1 Uso das informações para atividades de resposta a incidentes de segurança em redes de computadores	18,7	11,0	27,5	28,6	14,3	2,09
C2 Uso das informações para Suporte e atendimento aos usuários	13,2	14,3	18,7	29,7	24,2	2,37
C3 Uso das informações para atividades de resolução de problemas de *hardware, software*, sistemas de informação e redes	18,7	5,5	25,3	29,7	20,9	2,29
C4 Uso das informações para atividades de Aprendizado como preparação para resolver futuros problemas	6,6	12,1	28,6	29,7	23,1	2,51
C5 Uso das informações para aprimorar a segurança da informação na organização	4,4	15,4	22,0	31,9	26,4	2,60
C6 Uso das informações para auditoria em sistemas computacionais comprometidos	24,2	16,5	23,1	26,4	9,9	1,81
C7 Uso das informações para reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores	15,4	9,9	24,2	31,9	18,7	2,29

Fonte: elaboração própria

[a] No cálculo do Índice A (Média Ponderada), foram estabelecidos os seguintes pesos: 0 para Não utiliza; 1 para 1 vez ao ano; 2 para 1 vez ao mês; 3 para 1 vez na semana e 4 para 1 vez ao dia.

4.3.2 Pertinência

A Tabela 8 apresenta o uso da informação, em face da variável pertinência, com taxas mais elevadas e equilibradas do que as levantadas na Tabela 7 - Frequência.

Nesse aspecto, observa-se, de forma idêntica ao tabulado na tabela anterior, que o índice mais elevado coube ao quesito aprimoramento da segurança da informação no espaço cibernético inerente à organização com índice de 3,15 e uso diário por mais da metade dos respondentes. No outro extremo, a menor pertinência foi registrada nas atividades de auditoria em sistemas computacionais comprometidos com índice de 2,71.

Tabela 8 - Avaliação percentual da Pertinência por uso da informação

USO DA INFORMAÇÃO	Não utiliza (%)	1 vez ao ano %	1 vez ao mês %	1 vez na semana (%)	1 vez ao dia (%)	Índice A - SUBCATEGORIA ([a])
C1 Uso das informações para atividades de resposta a incidentes de segurança em redes de computadores	9,9	7,7	9,9	35,2	37,4	2,82
C2 Uso das informações para Suporte e atendimento aos usuários	6,6	9,9	12,1	35,2	36,3	2,85
C3 Uso das informações para atividades de resolução de problemas de *hardware, software*, sistemas de informação e redes	12,1	4,4	8,8	36,3	38,5	2,85
C4 Uso das informações para atividades de aprendizado como preparação para resolver futuros problemas	3,3	3,3	17,6	35,2	40,7	3,07
C5 Uso das informações para aprimorar a segurança da informação na organização	2,2	8,8	13,2	23,1	52,7	3,15
C6 Uso das informações para auditoria em sistemas computacionais comprometidos	14,3	4,4	16,5	25,3	39,6	2,71
C7 Uso das informações para reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores	6,6	6,6	13,2	24,2	49,5	3,03

Fonte: elaboração própria

[a] No cálculo do Índice A (Média Ponderada) foram estabelecidos os seguintes pesos: 0 para Não utiliza; 1 para 1 vez ao ano; 2 para 1 vez ao mês; 3 para 1 vez na semana e 4 para 1 vez ao dia.

4.3.3 Relacionamento entre Frequência e Pertinência

A partir das duas tabelas anteriormente mencionadas, foi realizado um cruzamento entre frequência e a pertinência do uso da informação, concretizado na Tabela 9.

Tabela 9 - Relacionamento entre Frequência e Pertinência

USO DA INFORMAÇÃO	Índice B - Frequência	Índice B - Pertinência	Variação entre Frequência e Pertinência
C1 Uso das informações para atividades de resposta a incidentes de segurança em redes de computadores	2,09	2,82	- 0,73
C2 Uso das informações para Suporte e atendimento aos usuários	2,37	2,85	- 0,48
C3 Uso das informações para atividades de resolução de problemas de *hardware, software*, sistemas de informação e redes da organização	2,29	2,85	- 0,56

C4 Uso das informações para atividades de Aprendizado como preparação para resolver futuros problemas	2,51	3,07	- 0,56
C5 Uso das informações para aprimorar a segurança da informação na organização	2,60	3,15	- 0,55
C6 Uso das informações para auditoria em sistemas computacionais comprometidos	1,81	2,71	- 0,90
C7 Uso das informações para reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores	2,29	3,03	- 0,74

Fonte: elaboração própria

Os usos identificados como de maior variação negativa entre os índices de frequência e pertinência, como pode ser percebido nos quesitos: Auditoria em sistemas computacionais comprometidos (- 0,90), Resposta a incidentes de segurança em redes de computadores (- 0,74) e Reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores (- 0,73), revelam que os mesmos podem estar sendo subestimados, necessitando de atenção especial nas organizações da APF.

Não obstante, as variações mais baixas obtidas pelas atividades: Suporte e atendimento aos usuários (- 0,48), Resolução de problemas de *hardware, software*, sistemas de informação e redes da organização (- 0,56) e Aprimorar a segurança da informação na organização (- 0,55) confirmam a predominância dos perfis estratégico e operacional dos respondentes.

4.4 Conclusões Parciais

O número de respondentes (91 alunos) ao questionário, correspondenteu a 22 % dos *e-mails* válidos enviados e geraram 6643 respostas, as quais foram complementadas pelos dados coletados nas entrevistas. Além dos formulários com as respostas, também foram recebidos alguns *e-mails* dos questionados, destacando-se positivamente a iniciativa e o formato da pesquisa. Tal fato, aliado às informações apuradas nas entrevistas, leva a crer que não houve dúvidas quanto ao preenchimento do questionário e quanto à pertinência e relevância dos dados.

A análise dos dados dessa pesquisa revela um importante conjunto de características do comportamento informacional de servidores e empregados de órgãos e entidades da administração pública federal, no tocante a segurança cibernética.

Essas características foram especialmente relativas: às necessidades de informação desses agentes, no desempenho de suas atividades, às fontes e canais de informação mais empregados, e aos usos dessa informação.

No capítulo seguinte, essas análises são discutidas à luz de literatura pertinente.

5 O COMPORTAMENTO INFORMACIONAL NA GESTÃO DA SEGURANÇA CIBERNÉTICA

5.1 Papéis desempenhados

Em relação aos pressupostos específicos do estudo (Seção 3.3.2), o primeiro afirma que o contexto situacional está diretamente relacionado com o papel desempenhado, na organização, pelo agente público que atua na segurança cibernética. Nesse caso, aflorou a necessidade do aperfeiçoamento técnico especializado, evidenciado pelo emprego nas atividades diárias dos conhecimentos obtidos por intermédio de pós-graduação *lato sensu,* das Certificações e cursos técnicos, que juntos alcançam expressivos 90% das respostas.

Ainda, no contexto do primeiro pressuposto específico, era esperada, pelo autor, uma divisão mais equânime entre os perfis pré-estabelecidos (estratégico, operacional e tático) em relação às tarefas primárias. Merece atenção o baixo número de respondentes (apenas 12%) que desempenham, primariamente, ações de gerenciamento de incidentes de segurança em redes de computadores, particularmente devido a três fatores de características distintas na essência, mas imbricadas na prática:

a) característica legal: publicação da Instrução Normativa n. 1, do Gabinete de Segurança Institucional da Presidência da República (IN 01/GSIPR), em 13 de junho de 2008 (Brasil, 2008a), que determinou a implementação de equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) em todos os órgãos da APF;
b) característica de conformidade: recomendações emitidas pelo TCU em 2010 e repetidas em anos posteriores sobre a gestão dos incidentes de segurança da informação e a instituição das ETIR (TCU, 2012, 2014b);
c) característica de Estado-nação: as repercussões das revelações do "caso Snowden" ocorrido em 2013, que, em âmbito nacional, entre outras medidas, levaram o Senado Federal brasileiro a instaurar uma Comissão Parlamentar de Inquérito (CPI) da Espionagem (SENADO FEDERAL, 2014).

5.2 Comportamento de busca da informação

No que tange ao segundo pressuposto específico - a análise do comportamento de busca é caracterizada pelas fontes e pelos canais utilizados no atendimento das necessidades de informação -, no relacionamento entre as variáveis utilizadas nessa avaliação (relevância, con-

fiabilidade e acessibilidade), destaca-se a subcategoria Publicações governamentais (normas, manuais), da categoria Impessoal Externa, que obteve os maiores índices nas três variáveis (3,49, 3,35 e 3,25, respectivamente). Destaca-se, também, que é prática comum a todos os respondentes consultar os mecanismos de busca na Internet (Google, Bing), como ressaltam os entrevistados:

> Hoje a maior fonte de informação é a Internet realmente. Raramente a gente vai buscar em livros, muitas vezes a gente consulta manuais, manuais de sistemas [...] a principal fonte de busca é o Google porque ele indexa tudo. Daí a gente vai buscando os *links* para outras fontes de informação. (Entrevista 3)

> [...] é buscado em várias fontes. Pode ser na Internet como os mecanismos de busca principais, uso muito o Google, ou as enciclopédias livres, tipo Wikipédia. (Entrevista 2)

Ainda no contexto da busca, os dados revelam que os agentes públicos envolvidos na segurança cibernética organizacional, consideram de maior relevância e confiabilidade as fontes de relacionamento Pessoal e de origem Interna à organização. Tal fato, também é corroborado pelo elevado índice de facilidade de acesso a essas fontes.

Assim sendo, esta pesquisa ratifica, parcialmente, o estudo realizado por Mafra Pereira e Barbosa (2008) onde, de forma semelhante, ficou demonstrado que os pesquisados, além de considerarem mais relevantes, confiam mais nas fontes pessoais (derivadas das suas redes de relacionamento) do que nas fontes impessoais. Dessa forma, a busca mais intensa por fontes de maior relevância e confiabilidade nas fontes pessoais demonstra que os responsáveis pela segurança da informação no espaço cibernético governamental, bem como os consultores do estudo de Mafra Pereira e Barbosa necessitam, para tomar decisões, de informações rápidas, de fácil acesso, mas que sejam ao mesmo tempo relevantes e confiáveis.

Pode-se inferir que o processo de busca da informação é realizado de maneira individual, ou seja, sem auxílio de terceiros. Dessa forma, foi confirmada a utilização da crença conhecida com Autoeficácia (*Self-efficacy),* oriunda do Modelo de Wilson (1997) e mantida na segunda fase dos mecanismos de ativação (teoria da Aprendizagem social) do Modelo de comportamento informacional para a gestão de segurança cibernética proposto no presente estudo. Nessa linha, pode-se afirmar que dos tipos de busca presentes no Modelo adotado, o mais comum refere-se à 'busca ativa' onde um indivíduo procura ativamente a informação de que necessita, e que, dependendo do resultado, pode ocasionar novas buscas. Nesse caso, não foram feitas, pelos entrevistados, alusões significativas a outros tipos de comportamento de busca da informação presentes no Modelo, como: atenção passiva, busca passiva e busca em andamento.

5.3 Usos da informação

No terceiro e último pressuposto específico - que remete à influência das tarefas diárias desempenhadas no ambiente de trabalho no uso da informação -, foram ratificados os usos mais frequentes e pertinentes da informação (Tabelas 7 e 8) com as tarefas prioritariamente realizadas (Gráficos 6 e 7).

Neste aspecto, observa-se que houve compatibilidade entre essas respostas, tendo em vista que os mais elevados índices de uso da informação, encontrados nos quesitos: aprimoramento da segurança da informação na organização e aprendizado como preparação para resolver futuros problemas, estão inseridos no perfil de cunho estratégico, declarado pela maioria dos questionados. Não obstante, cabe destacar que o quesito aprendizagem para resolver futuros problemas é compatível com os demais perfis.

Cabe destacar que, quando a diferença entre a frequência e a pertinência é mais significativa, afloram-se duas características peculiares no dia a dia do agente responsável pela segurança cibernética:

a) o uso das informações permanece focado e direcionado para atender às demandas do seu papel na organização, mesmo reconhecendo a importância e a utilidade da informação para a realização das atividades típicas de gestão de incidentes de segurança (como foi observado nos itens Resposta a incidentes de segurança em redes de computadores e Auditoria em sistemas computacionais comprometidos);
b) tendência a "apagar incêndios", colocando em segundo plano o uso pró-ativo da informação (de acordo com o analisado no quesito Reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores).

5.4 Modelo de comportamento informacional para a gestão de segurança cibernética

Buscou-se analisar o comportamento informacional dos agentes públicos que atuam na gestão da segurança cibernética governamental, por intermédio do modelo de comportamento informacional de Wilson (1997), o qual foi adaptado pelo autor, durante a etapa de revisão da literatura, servindo de esteio para a realização desta pesquisa.

Cabe ressaltar que, após as fases de coleta e de análise dos dados, foi percebida a necessidade de ajustes oriundos da realidade observada mediante as respostas dos questionários e das entrevistas. Dentre as alterações mais significativas realizadas, destacam-se:

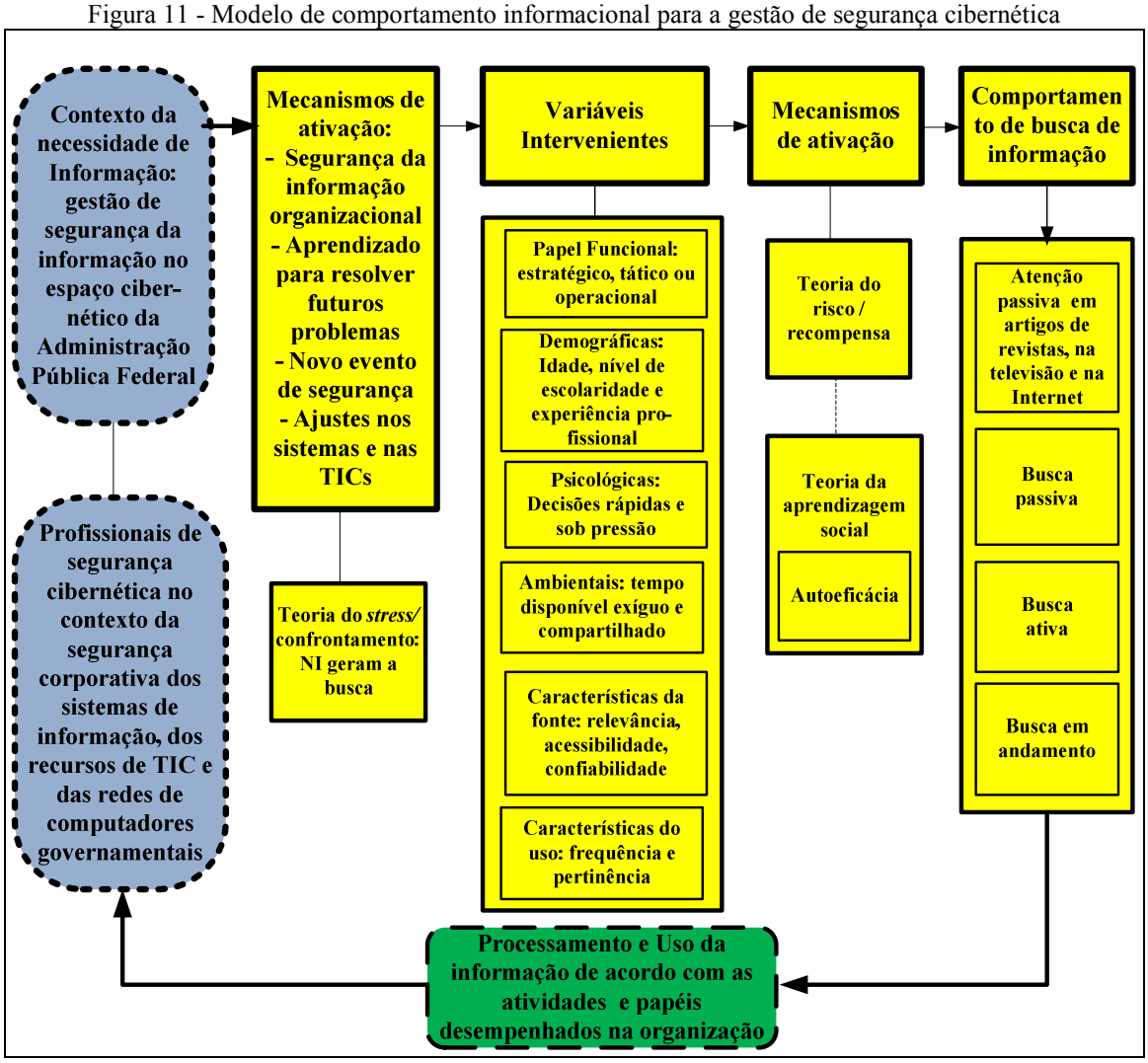
a) a utilização das três perspectivas de atuação propostas pelo autor: nível estratégico, nível operacional ou nível tático;

b) a inserção de mecanismos de ativação relacionados com as atividades e os papéis desempenhados na organização;

c) a caracterização das variáveis intervenientes.

Dessa forma, o Modelo de comportamento informacional adaptado (Figura 7) foi customizado ao longo do estudo, como apresentado na Figura 11 a seguir.

Figura 11 - Modelo de comportamento informacional para a gestão de segurança cibernética



Fonte: elaboração própria

6 CONCLUSÕES, LIMITAÇÕES E SUGESTÕES

6.1 Conclusões do estudo

O objetivo geral deste estudo foi analisar o comportamento informacional dos agentes públicos que atuam na gestão da segurança cibernética governamental, no âmbito da Administração Pública Federal. Dessa forma, a fim de delimitar o percurso a ser adotado na pesquisa, foram definidos objetivos com vistas a: (1) identificar as fontes e os canais mais relevantes, confiáveis e acessíveis, (2) os usos mais frequentes e pertinentes da informação e (3) mapear tendências do comportamento informacional de um grupo representante de agentes públicos, quando envolvidos na segurança cibernética na APF.

A partir, portanto, da análise dos dados obtidos pelos instrumentos de coleta alinhados às demandas dos objetivos da pesquisa (Quadro 9 - Relacionamento entre os OE e os dados da pesquisa, p. 62), foi possível, em resumo, identificar:

a) predominância de atuação no nível estratégico por parte dos agentes públicos envolvidos com segurança cibernética;
b) importância da pós-graduação *lato sensu,* das Certificações e dos cursos técnicos de curta duração nas atividades de segurança da informação no espaço cibernético;
c) equilíbrio na relevância das fontes/canais Pessoal Interno e Impessoal Externo;
d) maior confiabilidade e facilidade de acesso às fontes/canais pessoais e internas à organização;
e) uso mais frequente e pertinente das informações refere-se às atividades desenvolvidas com a finalidade de aprimorar a segurança da informação na organização;
f) oportunidades de melhoria nas atividades relativas à gestão de incidentes de segurança caracterizada pelo baixo percentual de agentes públicos que atuam prioritariamente nessa área e pela significativa discrepância (baixa frequência *versus* alta pertinência) em relação ao uso das informações.

Assim sendo, a presente pesquisa almejou contribuir para a melhoria quanto ao desempenho dos responsáveis por gerir a segurança da informação no espaço cibernético inerente à Administração Pública Federal brasileira, fornecendo subsídios para o aperfeiçoamento e o planejamento de iniciativas de compartilhamento e disponibilização de informações relevantes, confiáveis e pertinentes para a segurança cibernética, no âmbito das instituições governamentais.

6.2 Contribuições do estudo

No contexto epistemológico da interdisciplinaridade inerente à Ciência da informação, particularmente do Estudo de Usuários, o estudo ora realizado corrobora os dois tipos de necessidades de informação, considerados importantes por Figueiredo (1994): a necessidade de informação em função do conhecimento (que resulta do desejo de saber) e a necessidade de informação em função da ação (que resulta de necessidades materiais exigidas para a realização de atividades humanas, profissionais e pessoais), apesar do distanciamento temporal de três décadas e os substanciais avanços das TICs.

Ainda neste contexto, acredita-se que o Modelo de comportamento informacional para a gestão de segurança cibernética, adaptado de Wilson, possa ser utilizado em estudos posteriores sobre os temas: segurança da informação no espaço cibernético (segurança cibernética) e defesa cibernética.

Extrapolando o contexto epistemológico, sob o viés prático da CI, a presente pesquisa reforça, nos profissionais de informação, a viabilidade e importância do desenvolvimento e aperfeiçoamento dos sistemas de informações (P.ex.: enciclopédias virtuais tipo *wiki*), bem como o uso das mídias sociais (fóruns, *chats*, listas, *blogs*) internas à Organização.

No macroambiente político-social da segurança da informação no espaço cibernético nacional, observou-se significativa dependência na utilização de mecanismos de buscas estrangeiros para solução das situações-problemas de segurança cibernética. Tais mecanismos, como Google e Bing, além de não possuírem acordos formais de uso com o estado brasileiro, podem interromper, manipular e monitorar a busca de informações pelos agentes públicos, podendo comprometer a segurança de uma área tão sensível da APF.

Ainda em relação ao macroambiente político-social, acredita-se que este estudo possa contribuir para a implantação de medidas visando à potencialização da Defesa Cibernética Nacional, particularmente no que tange ao projeto de criação da Escola Nacional de Defesa Cibernética - ENaDCiber[39] (BRASIL, 2014a).

[39] ENaDCiber é uma iniciativa do Ministério da Defesa e tem como objetivo criar uma "célula nacional", capaz de absorver e disseminar as capacitações relativas à defesa cibernética. Isto, por sua vez, reduziria as lacunas nas áreas de pesquisa, desenvolvimento, operação e gestão relativas à segurança e à defesa cibernética nos níveis de sensibilização, conscientização, formação e especialização.

6.3 Limitações do estudo

Pode-se considerar uma das limitações do estudo, a utilização dos alunos do Curso de Especialização em Gestão da Segurança da Informação e Comunicações, principalmente no que tange a quantidade de agentes públicos responsáveis pela segurança do espaço cibernético na APF. Assim sendo, os dados analisados pertencem a uma amostra (alunos do CEGSIC) que permeia, parcialmente, o universo da pesquisa. Acredita-se que, para uma pesquisa de mestrado, onde foi utilizada a seleção da amostra por acessibilidade, o número de respondentes atingiu os objetivos desejados.

Tal limitação, entretanto, deriva-se da forma escolhida para superar as dificuldades técnicas relacionadas ao mapeamento de todos os possíveis agentes públicos envolvidos com segurança cibernética, os quais estão distribuídos por dezenas de órgãos da APF em todo o território nacional.

Não obstante, a amostra possui características peculiares (P.ex.: habilitação para realizar um curso de pós-graduação) que podem ter influenciado, particularmente, os resultados referentes à Idade e Formação Acadêmica. Dessa forma, os valores percentuais, bem como os Índices A e B produzidos, expressam **tendências** do comportamento informacional na gestão da segurança cibernética na APF.

6.4 Sugestões para estudos futuros

O autor considera importante aprofundar os estudos sobre o comportamento informacional dos agentes que realizam a segurança cibernética da APF, utilizando os três níveis propostos (estratégico, tático e operacional), particularmente no que se refere ao emprego *in loco* da informação obtida. Tal se justifica porque não foi objeto da presente pesquisa a aferição do uso eficaz da informação adquirida, durante o processo de busca da informação para auxiliar na solução da situação-problema. Neste contexto, sugere-se, também, o aprofundamento deste estudo por outras metodologias como a análise documental ou a atuação dos agentes públicos em "incidentes críticos".

Também se julga oportuno, estudar as causas e os motivos que norteiam as preferências em relação ao comportamento informacional dos referidos agentes, identificando-se os principais fatores que contribuem para que ocorram as tendências levantadas nesta pesquisa ou mesmo, em pesquisas futuras.

Em relação ao modelo proposto, sugere-se que, a fim validar as tendências levantadas, o mesmo seja aplicado em outras amostras representativas dos responsáveis pela gestão da segurança cibernética na APF. Não obstante, o modelo poderia ser aplicado no âmbito dos poderes Legislativo e Judiciário, em outras esferas governamentais do poder executivo (estados e municípios), bem como nas instituições relacionadas às infraestruturas críticas nacionais, públicas ou privadas.

Ainda, como sugestão de futuros estudos, poderia ser discutida a organização das informações, diretamente relacionadas com a segurança e a defesa do espaço cibernético, no contexto da Administração Pública Federal brasileira.

REFERÊNCIAS

ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO. **Introdução à Segurança da Informação** - Microsoft TechNet, 2006. Disponível em: <http://www.nerdbb.com/download/file.php?id=2618>. Acesso em: 01 abr. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27002:2013 - **Tecnologia da informação** - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ALVES, Alda Judith. A "revisão da bibliografia" em teses e dissertações: meus tipos inesquecíveis. **Cadernos de Pesquisa**, São Paulo, n. 81, p. 53-60, maio 1992. Disponível em: <http://www.fcc.org.br/pesquisa/publicacoes/cp/arquivos/916.pdf>. Acesso em: 23 fev. 2014.

ANSOFF, H. I. **A nova estratégia empresarial**. São Paulo: Atlas, 1990.

ARAÚJO, Carlos Alberto Ávila. Abordagem interacionista de estudos de usuários da informação. **Ponto de Acesso**, v. 4, n. 2, p. 02-32, 2010. Disponível em <http://www.portalseer.ufba.br/index.php/revistaici/article/view/3856>. Acesso em: 01 mar 2014.

BALLESTERO-ALVAREZ, M. E. **Manual de organização, sistemas e métodos**: abordagem teórica e prática a engenharia da informação. São Paulo: Atlas, 1997.

BAPTISTA, S. G., CUNHA, M. B. Estudos de Usuários: Visão Global dos Métodos de Coleta de Dados. **Perspectiva em Ciência da Informação**, Belo Horizonte, v. 12, n. 2, p. 168-184, maio/ago. 2007.

BARBOSA, Ricardo Rodrigues. Acesso e necessidades de informação de profissionais brasileiros: um estudo exploratório. **Perspectiva em Ciência da Informação**, Belo Horizonte, v. 2, n. 1. p. 5-35, jan./jun. 1997. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/32>. Acesso em: 21 mar. 2014.

BARDIN, Laurence. **Análise de Conteúdo**. Lisboa: Edições 70, 2009.

BASTOS, Jaime S. Y. O uso de fontes de informação por executivos do setor de tecnologia da informação. **Encontro Nacional de Pesquisa em Ciência da Informação** (Enancib), Florianópolis, 2005.

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 27002**: gestão de segurança da informação - uma visão prática. Porto Alegre, RS: Zouk, 2009.

BEZERRA, E. K. **Gestão de riscos de TI**: NBR 27005. Rio de Janeiro: RNP/ESR, 2011.

BORKO, H. Information science: what is it? **American Documentation**, v. 19, n. 1, 1968.

BRANTLEY, B. Elaboração de questionários e formulários. In: MALHOTRA, N. K. **Pesquisa de marketing; uma orientação aplicada.** 4. ed. Porto Alegre: Bookman, 2006. p. 273-298.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSIPR n. 1, de 13 de junho de 2008. **Disciplina a gestão da segurança da informação e comunicações na administração pública federal, direta e indireta e dá outras providências.** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 13 de junho de 2008a, n. 115 - Seção 1**.**

_____. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar n. 05/IN01/DSIC/GSIPR. **Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 17 de agosto de 2009a, n. 156 - Seção 1.

_____. Gabinete de Segurança Institucional da Presidência da República. Portaria n. 45, de 8 de setembro de 2009b. **Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências.** Disponível em <http://www.in.gov.br/visualiza/index.jsp?data=09/09/2009&jornal=1&pagina=2&totalArquivos=80>. Acesso em: 10 maio 2013.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas – MD35-G-01**. Apresenta definições de termos comuns às Forças Armadas. Brasília, 2007. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf>. Acesso em: 09 jun. 2013.

_____. Ministério da Defesa. **Doutrina de Operações Conjuntas – MD30-M-01.1.** v. 1 Brasília, 2011. Disponível em: <https://www.defesa.gov.br/arquivos/File /legislacao/emcfa/publicacoes/md_30_m_01_1volume.pdf> Acesso em: 09 jun. 2013.

_____. Ministério da Defesa. Portaria normativa n. 2.777, de 27 de outubro de 2014. **Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências**. Diário Oficial[da] República Federativa do Brasil. Brasília, DF, 2014a. Disponível em: <http:// http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=7&data=28/10/2014>. Acesso em: 29 out. 2014.

BRASIL. Presidência da República. Decreto n. 3.505, de 13 de junho de 2000. **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal**. Diário Oficial[da] República Federativa do Brasil. Brasília, DF, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 29 out. 2013.

_____. Presidência da República. Decreto n. 5.484, 30 de junho de 2005. **Política de Defesa Nacional.** Diário Oficial[da] República Federativa do Brasil**.** Brasília, DF, 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 21 jan. 2014.

_____. Presidência da República. Decreto n. 6.703, de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa, e dá outras providências**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008b.

_____. Presidência da República. Decreto n. 8.135, de 4 de novembro de 2013. **Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.prova a Estratégia Nacional de Defesa, e dá outras providências**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 5 de novembro de 2013.

BRASIL. Tribunal de Contas da União - TCU. Acórdão n. 2585/2012 – TCU – Plenário. **Relatório de Levantamento.** Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2012. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367>. Acesso em: 29 nov. 2014.

_____. Acórdão n. 3117/2014 – TCU – Plenário. **Relatório de Levantamento**. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2014b. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc>. Acesso em: 01 dez. 2014.

CALVA GONZÁLEZ, Juan J. **El fenómeno de las necesidades de información**: su investigación y modelo teórico. México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas, 2007. Disponível em: <http://libros.metabiblioteca.org/bitstream/001/400/8/970-32-4108-5.pdf>. Acesso em: 02 mar. 2014.

CAMPELO, Bernadete S.; CALDEIRA, Paulo da T (Orgs.). **Introdução às fontes de informação.** Belo Horizonte: Autêntica Editora, 2005.

CAPURRO, Rafael. Epistemologia e ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 5., 2003, Belo Horizonte. [**Anais]** do Encontro**...** Belo Horizonte: Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação e Biblioteconomia, 2003. Disponível em <http://www.capurro.de/enancib_p.htm>. Acesso em: 02 mar. 2014.

CASADO, Elias S. **Manual de Estudios de Usuarios**. Fundación Germán Sánchez Ruipérez. Madrid: Pirámide, 1994.

CASE, Donald O. **Looking for Information**: A Survey of Research on Information Seeking, Needs, and Behavior. San Diego: Elsevier Academic Press, 2002.

_____. Information Behavior. **Annual Review of Information Science and Technology**, v. 40, p. 293-327, 2006.

CAVALCANTI,C. R. de O. CUNHA, M. B. da. **Dicionário de biblioteconomia e arquivologia.** Brasília: Briquet de Lemos, 2008.

CEGSIC 2012/2014. **Seleção de candidatos para oferta de vagas em Curso de Pós- Graduação Lato Sensu.** Edital n. 6. Brasília, 2013. Disponível em: <https://selecao.cegsic.unb.br/12_14/mod/forum/discuss.php?d=3>. Acesso em: 30 mar. 2014.

CENDÓN, B. V.. A Internet. In: CAMPELLO, B. S.; CENDÓN, B. V.; KREMER, J. M. (Orgs.). **Fontes de informação para pesquisadores e profissionais.** Belo Horizonte: UFMG, 2000. p. 280-288.

CENDÓN, B. V.; ROLIM, E. A. Modelos teóricos de estudos de usuários na ciência da informação. **DataGrama Zero - Revista de Informação**, Rio de Janeiro, v. 14, n. 2, abr. 2013. Disponível em: < http://www.dgz.org.br/abr13/Art_06.htm>. Acesso em: 02 mar. 2014.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para a Internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em:<http://cartilha.cert.br/>. Acesso em: 29 out. 2013.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA Roberto da. **Metodologia Científica.** 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CHIAVENATO, Idalberto. **Introdução à Teoria geral da Administração:** uma visão abrangente da moderna administração das organizações. 7. ed. Rio de Janeiro: Elsevier, 2003.

CHOO, Chun Wei. Perception and use of information sources by chief executives in environmental scanning. **Library and Information Science Research**. v. 16, p.23-40, 1994.

_____. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. 2. ed. São Paulo: SENAC, 2006.

_____. **The knowing organization**: how organizations use information to construct meaning, create knowledge and make decisions. London: Oxford University Press, 2007.

CISCO. **Cisco 2014 Annual Security Report.** Cisco Systems, Inc. San Jose, CA, 2014. Disponível em: < https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf >. Acesso em: 10 jun. 2014.

CLARKE, Richard A; KNAKE, Robert **Cyber War**: The Next Threat to National Security and What to Do About It. New York: Harper Collins publisher, 2010.

CONSELHO NACIONAL DE ARQUIVOS - Conarq (Brasil). **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro : Arquivo Nacional, 2011.

CRESWELL, John W. P**rojeto de pesquisa**: método qualitativo, quantitativo e misto. 2. ed. Porto Alegre: Artmed, 2007.

CRESWELL, J. W.; CLARK, V. L. **Designing and conducting mixed methods research**. Thousand Oaks: Sage, 2007.

CUNHA, M. B. da. Metodologias para estudo dos usuários de informação cientifica e tecnológica. **Revista de Biblioteconomia de Brasília**, v. 10, n. 2, p. 5-19, jul./dez. 1982.

DAVENPORT, Thomas H.; PRUSAK, Laurence. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DEMO, P. Metodologia científica em ciências sociais. São Paulo: Atlas, 1995.

DERVIN, Brenda; NILAN, Michael. Information needs and uses. **Annual Review of Information Science and Technology**, v. 21, p. 03-33. 1986.

EJOURNAL USA. **Estônia Torna-se E-stônia.** Departamento de Estado dos EUA, v. 15 n. 6, jun. 2010. Disponível em: <http://www.embaixada-americana.org.br/HTML/ijse0610p/estonia.h>. Acesso em: 22 jan. 2014.

ELIAS, Paulo Sá. A tecnologia e o Direito no século XXI: nova abordagem. **Jus Navigandi**, Teresina, ano 7, n. 53, jan. 2002. Disponível em: <http://jus.com.br/artigos/2547>. Acesso em: 24 out. 2014.

FERNANDES, Jorge H. C. **A Organização e a Tecnologia da Informação**: Sistemas de Informações, Infraestrutura, Organização e Serviços, 2009. Disponível em: <http://www.cpd.unb.br/images/A_Organizacao_e_a_Tecnologia_da_Informacao.pdf>. Acesso em: 20 jul. 2014.

_____. **Segurança da Informação:** nova disciplina da Ciência da Informação**?** In: XI E-NANCIB - Encontro Nacional de Pesquisa em Ciência da Informação. Brasília: Universidade de Brasília, 2010. Disponível em: <http://enancib.ibict.br/index.php/xi/enancibXI/paper/viewFile/527/210>. Acesso em: 22 jan. 2014.

_____. **Relatório do curso de Especialização em Gestão da Segurança da Informação e Comunicações**. Brasília: Universidade de Brasília - Decanato de Pesquisa e Pós-graduação, 2012a.

_____. **Segurança e Defesa Cibernéticas para Reduzir Vulnerabilidades nas Infraestruturas Críticas Nacionais (Relatório Técnico).** Núcleo de Estudos Prospectivos do Exército Brasileiro. Brasil: Exército Brasileiro, 2012b. 46 p. Disponível em: <http://www.eme.eb.mil.br/ceeex/public/arquivos/nep2012/NEP_CEEEx_Jorge_Fernandes_2012.pdf>. Acesso em: 22 jan. 2014.

FIGUEIREDO, Nice Menezes. **Estudos de uso e usuários da informação**. Brasília: IBICT, 1994.

FREITAS, W. L. de; GOMES, U. M.; RÊGO BARROS, O. S. (Orgs.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

GASQUE, Kelley; COSTA, Sely M. de S. **Evolução teórico-metodológica dos estudos de comportamento informacional de usuários.** Ciência da Informação, Brasília, v. 39, n. 1, p. 21-32, jan./abr. 2010.

GIL, Antônio Carlos. **Métodos e técnicas em pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GOVERNO ELETRÔNICO. **Apresenta notícias, eventos, fórum de discussão e amparos legais.** Disponível em: <http://www.governoeletronico.gov.br/>. Acesso em: 29 mar. 2014.

ISO/IEC. **ISO/IEC 27000** - Information technology - Security Techniques - Information security management systems - Overview and vocabulary. 2014.

ISO/IEC. **ISO/IEC 27032** - Information technology - Security Techniques - Guidelines for cybersecurity. 2012.

KLIMBURG, Alexander. **National Cyber Security Framework Manual**. Talinn: NATO CCD COE Publication, 2012.

KOTLER, P. **Administração de marketing**: a edição do novo milênio. São Paulo: Prentice Hall, 2000.

LAKATOS, E. M.; MARCONI, M. A. Fundamentos da metodologia científica. 7. ed. São Paulo: Atlas, 2010.

LE COADIC, Y. F. **A Ciência da Informação**. Brasília: Briquet de Lemos, 1996.

_____. **Le besoin d'information**. Paris: ADBS Editions, 1998.

_____. Princípios científicos que direcionam a ciência e a tecnologia da informação digital. **Transinformação**, Campinas, v. 16, n. 3, p. 205-213, set./dez. 2004.

LÉVY, Pierre. **O que é o virtual?** São Paulo: Editora 34, 1996.

LOPEZ, André Ancona Porto. Diretrizes para o Desenvolvimento de Projetos de Cunho Científico. Brasília: CEGSIC, 2010.

LIMA-MARQUES, M.; MARCIANO, J. L. O enfoque social da segurança da informação. **Ciência da Informação**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. Disponível em: <http://www.scielo.br/pdf/ci/v35n3/v35n3a09.pdf>. Acesso em 03 mar. 2014.

LINS, Greyciane Souza. **Colaborações dos estudos de cibercultura para a ciência da informação.** Brasília, 2013. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2013.

MACINTOSH-MURRAY, Anu; CHOO, Chun Wei. Information failures in health Care. Annual Review of Information Science and Technology, v.40, p. 357-391, 2006.

MAFRA PEREIRA, Frederico Cesar; BARBOSA, Ricardo Rodrigues. Uso de fontes de informação por consultores empresariais: um estudo junto ao mercado de consultoria de Belo Horizonte. Perspectiva em Ciência da Informação, v. 13, n. 1. p. 95-111, jan./abr., 2008. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/163/421>. Acesso em: 21 mar. 2014.

MARCIANO, J. L. Segurança da Informação - Uma Abordagem Social. Brasília, 2006. Tese (Doutorado em Ciências da Informação) - Universidade de Brasília. Brasília, 2006.

MARQUES, Anna. Maria de O.; WALLIER VIANNA, Eduardo. Identificação das necessidades de informação dos profissionais de segurança da informação. **Revista Tecnologias em Projeção**, v. 4, n. 2, dez., 2013. Disponível em:

<http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/321/240>. Acesso em: 02 mar. 2014.

MARTINEZ-SILVEIRA, Martha; ODDONE, Nanci**.** Necessidades e comportamento informacional: conceituação e modelos. **Ciência da Informação**, Brasília, v. 36, n. 2, ago., 2007. Disponível em < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652007000200012&lng=pt&nrm=iso&tlng=pt>. Acesso em: 02 mar. 2014.

MINAYO, Maria C. de S. (Org). **Pesquisa social**: teoria, método e criatividade. 26. ed. Petrópolis: Vozes, 2007.

MIRANDA, Silvana. Como as Necessidades de Informação podem se Relacionar com as Competências Informacionais. **Ciência da Informação**, Brasília, v.35, n.3, p.99-144, set/dez 2006. Disponível em: <http://www.scielo.br/pdf/ci/v35n3/v35n3a10.pdf>. Acesso em: 02 mar. 2014.

_____. **Identificação de necessidades de informação e sua relação com as competências informacionais**: o caso da supervisão indireta de instituições financeiras no Brasil. Brasília, 2007. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2007. Disponível em: <http://repositorio.unb.br/handle/10482/2903>. Acesso em: 02 mar. 2014.

MORESI, Eduardo. **Metodologia da Pesquisa.** Brasília: Universidade Católica de Brasília, 2003.

NIC.br - Núcleo de Informação e Coordenação do ponto br. **Dimensões e Características da Web Brasileira**: um estudo do gov.br**.** Brasil, 2010. Disponível em: < http://www.cgi.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-da-informacao-e-da-comunicacao-no-brasil-tic-governo-eletronico-2010/>. Acesso em: 29 nov. 2014.

NYE, Joseph S. **O futuro de poder.** São Paulo: Benvirá, 2012.

OLSON, Soren. **"**Treino de Sombra**":** a Guerra Cibernética e o ataque econômico estratégico*,* **Military Review brasileira,** Kansas, set.-out., 2012. p. 73-83.

OHTOSHI, Paulo Hideo. **O comportamento informacional:** estudo com especialistas em segurança da informação e criptografia integrantes da RENASIC/COMSIC Brasília, 2013. Dissertação (Mestrado em Ciência da Informação) - Universidade de Brasília, Brasília, 2013.

RAMOS, Anderson et al. (Orgs.). **Security Officer – 1:** Guia Oficial para Formação de Gestores em Segurança da Informação**.** 2. ed., Porto Alegre, RS: Zouk, 2006.

RUSTICI, Ross M. **Armas Cibernéticas**: Igualando Condições no Âmbito Internacional*,* **Military Review brasileira,** Kansas, jul-ago, 2012. p. 61-70.

SACERDOTE, Helena Célia de Souza. **Análise da mediação em educação online sob a ótica da Análise de Redes Sociais**: o caso do curso de Especialização em Gestão da Segurança da Informação e Comunicações. Brasília, 2013. Dissertação (Mestrado em Ciência da Informação) - Universidade de Brasília, Brasília, 2013.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, v. 1, n. 1, p. 41-62, jan./jun., 1996. Disponível em: <http:// http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235>. Acesso em: 02 mar. 2014.

_____. **Information science**. In: Encyclopedia of Library and Information Science. New York: Taylor & Francis, 2009. p. 2570-2586. Disponível em: <http://comminfo.rutgers.edu/~tefko/SaracevicInformationScienceELIS2009.pdf>. Acesso em: 20 jun. 2014.

SENADO FEDERAL. **Em Discussão!**. Brasília, n.21, jul. 2014. Disponível em: <http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/>. Acesso em: 29 nov. 2014.

SHAKARIAN, Paulo. Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008*,* **Military Review brasileira,** Kansas*,* nov.-dez., 2011. p. 68-73.

VIDAL, F B; FERNANDES, J H C. **Segurança Física e do Ambiente** (notas de aula). Campus Universitário Darcy Ribeiro; Brasília - DF: Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / Departamento de Ciência da Computação; Instituto de Ciências Exatas; Universidade de Brasília, 2013. p. 39.

WALLIER VIANNA, Eduardo. **Procedimentos para a gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal**. Monografia (Especialização em Gestão de Segurança da Informação e Comunicações) - Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2011. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/16_Eduardo_Wallier.pdf>. Acesso em: Acesso em: 29 out. 2013.

_____. A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável. In: NAKAIAMA M. K. et al. (Orgs.). **Ciência, tecnologia e inovação**: pontes para a segurança pública. Florianópolis: FUNJAB, 2013a. cap. 5. p. 127-156.

_____. **Procedimentos para a gestão da segurança da informação em redes de computadores**. In: IX Workshop Internacional em Ciência da Informação - WICI 2013. Faculdade de Ciência da Informação, Universidade de Brasília, 2013b.

WALLIER VIANNA, E.; FERNANDES, J H C. **O gestor da segurança da informação no espaço cibernético governamental**: grandes desafios, novos perfis e procedimentos, 2014. (Submetido/aceito pelo periódico Brazilian Journal of Information Science: research trends, aguardando publicação).

WIENER, Norbert. **Cibernética e a sociedade**: o uso humano dos seres humanos. 2. ed, São Paulo: Cultrix, 1968.

_____. **Cybernetics – 2nd Edition**: or the control and Communication in the animal and the machine. EUA: MIT Press, 1995.

WILSON, Thomas. D. On user studies and information needs. **Journal of Librarianship,** n. 37, v. 1, p. 3-15, 1981. Disponível em: <http://informationr.net/tdw/publ/papers/1981infoneeds.html>. Acesso em: 18 mar. 2014.

_____. Information behaviour: an InterDisciplinary Perspective. **Information Processing & Management**, v. 33, n. 4, p. 551-572, 1997. Disponível em: <http://ptarpp2.uitm.edu.my/silibus/infoBehavior.pdf>. Acesso em: 22 jun. 2014.

_____.Models in information behaviour research. **Journal of Documentation**, v. 55, n. 3, p. 249-270, 1999. Disponível em: <http://informationr.net/tdw/publ/papers/1999JDoc.html>. Acesso em: 02 mar. 2014.

_____. Recent trends in user studies research and qualitative methods. **Information Research**, v. 5, n. 3, mar., 2000a. Disponível em: <http://www.informationr.net/ir/5-3/paper76.html>. Acesso em: 18 mar. 2014.

_____. Human Information Behavior. **Informing Science**, v. 3, n. 2, p. 49-55, 2000b. Disponível em: <http://ptarpp2.uitm.edu.my/ptarpprack/silibus/is772/humaninfobehavior.pdf>. Acesso em: 02 mar. 2014.

_____. **Philosophical foundations and research relevance**: issues for information research. Fourth International Conference on Conceptions of Library and Information Science: Emerging Frameworks and Method, University of Washington, Seattle, jul. 2002a. Disponível em: <http://informationr.net/tdw/publ/papers/COLIS4.html>. Acesso em: 18 mar. 2014.

_____. The nonsense of knowledge management. **Information Research,** v. 8, n. 1, Oct 2002b. Disponível em: <http://InformationR.net/ir/8-1/paper144.html>. Acesso em: 18 mar. 2014.

_____. A problemática da gestão do conhecimento. In: TARAPANOFF, K. (orgs). **Inteligência, informação e conhecimento em corporações.** Brasília: IBICT/UNESCO, 2006. p. 37-55.

WILSON, Thomas D.; WALSH, C. Information behaviour: an inter-disciplinary perspective. **British Library Research and Innovation Report,** n. 10, 1996. Disponível em: <http://www.informationr.net/tdw/publ/infbehav/>. Acesso em: 22 jun. 2014.

ZINS, Chaim. Knowledge map of information science: Research Articles**. Journal of the American Society for Information Science and Technology**, n. 58, v.4, p.526-535, 2007.

APÊNDICE A - Questionário

Universidade de Brasília

Programa de Pós-Graduação em Ciência da Informação

Prezado (a) Senhor (a),

Sou mestrando na Faculdade de Ciência da Informação da Universidade de Brasília, e solicito sua colaboração em participar de um questionário. A pesquisa é sobre comportamento informacional e pretendo avaliar as necessidades, as fontes de informação, a busca e o uso da informação pelos profissionais que atuam na segurança cibernética no âmbito da Administração Pública Federal (APF).

Considera-se que segurança cibernética encontra-se inserida no contexto da segurança da informação e pode ser definida como: a preservação da confidencialidade, da integridade e da disponibilidade da informação na Internet, incluindo não somente o *hardware, software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes.

O questionário está dividido em três blocos:

1º Bloco: identificação do perfil e do contexto das necessidades de informação;

2º Bloco: avaliação dos principais canais e fontes de informação;

3º Bloco: uso da informação no desempenho das suas atividades no seu ambiente de trabalho/Organização.

Estima-se que serão necessários 20 minutos para respondê-lo.

Antecipadamente agradeço sua preciosa colaboração

Cordialmente

Eduardo Wallier Vianna
Mestrando da Faculdade de Ciência da Informação - UnB (e ex-aluno do CEGSIC)

Jorge Henrique Cabral Fernandes
Orientador - Professor Doutor - Faculdade de Ciência da Informação - UnB.

Editar este formulário

Universidade de Brasília

Programa de Pós-Graduação em Ciência da Informação

Comportamento informacional dos profissionais que atuam na segurança cibernética no âmbito da APF.

*Obrigatório

A1 Sexo *

- FEMININO
- MASCULINO

1º BLOCO -IDENTIFICAÇÃO DO PERFIL E DO CONTEXTO DAS NECESSIDADES DE INFORMAÇÃO

A2 Idade *

- até 25 anos
- 25 a 29 anos
- 30 a 39 anos
- 40 a 49 anos
- mais de 50 anos

A3 Tempo de experiência como profissional de segurança cibernética, ou seja, relacionado a preservação da confidencialidade, da integridade e da disponibilidade da informação na internet, incluindo não somente o hardware, software e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes *

- até 1 ano
- 1 a 2 anos
- 3 a 4 anos
- mais de 5 anos

A4 Tempo de trabalho como profissional de segurança cibernética na 'sua' Organização / Instituição *

- até 1 ano

- 1 a 2 anos
- 3 a 4 anos
- mais de 5 anos

A5 Formação acadêmica mais elevada concluída *

- Graduação
- Pós-Graduação Latu Sensu (Especialização, MBA)
- Mestrado (acadêmico ou profissional)
- Doutorado

A6 Qual a 'sua' formação/capacitação/curso MAIS RELEVANTE/UTILIZADA na área de segurança cibernética? *

- Graduação
- Pós-Graduação Latu Sensu (Especialização, MBA)
- Mestrado (acadêmico ou profissional)
- Doutorado
- Certificações (CompTIA, CISM, CISSP, outras)
- Outros cursos (Cert/NIC.br, ESR/RNP etc)

A7 No desempenho das suas tarefas cotidianas ou diárias, relacionadas à segurança cibernética, você mais necessita de informações para realizar, PRIMARIAMENTE: *

- Coordenação, planejamento e gestão de alto nível para alcançar resultados de longo prazo, referentes à gestão de continuidade, gestão de riscos, políticas de segurança organizacionais etc
- Contato direto com sistemas computacionais, de controle ou rede de computadores, visando configuração, operação etc
- Triagem, análise, tratamento e resposta a incidentes de segurança em redes de computadores

A8 No desempenho das suas tarefas cotidianas ou diárias, relacionadas à segurança cibernética, você mais necessita de informações para realizar, SECUNDARIAMENTE: *

- Coordenação, planejamento e gestão de alto nível para alcançar resultados de longo prazo, referentes à gestão de continuidade, gestão de riscos, políticas de segurança organizacionais etc
- Contato direto com sistemas computacionais, de controle ou rede de computadores, visando configuração, operação etc
- Triagem, análise, tratamento e resposta a incidentes de segurança em redes de computadores

Continuar »

33% concluído

Editar este formulário

Universidade de Brasília

Programa de Pós-Graduação em Ciência da Informação

Comportamento informacional dos profissionais que atuam na segurança cibernética no âmbito da APF.

*Obrigatório

2º BLOCO: CANAIS E FONTES DE INFORMAÇÃO

Utilizados no desempenho das suas atividades como profissional de segurança cibernética, ou seja, relacionadas a preservação da confidencialidade, da integridade e da disponibilidade da informação na internet, incluindo não somente o hardware, software e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes no seu ambiente de trabalho/Organização.

Cada fonte ou canal deverá ser avaliado numericamente e de forma crescente de 1 (menor) a 4 (maior), de acordo com sua Relevância, Confiabilidade e Facilidade de Acesso:

1 para Irrelevante / Pouco confiável / Muito Difícil o Acesso
2 para Pouco Relevante / Pouco Confiável / Difícil Acesso
3 para Relevante / Confiável / Acessível
4 para Muito relevante / Muito Confiável / Fácil Acesso
e 0 (zero) caso não utilize a fonte ou canal.

B1 Encontros oficiais EXTERNOS à organização (seminários, congressos etc.) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B2 Conversa com fornecedores, consultores e outros, EXTERNOS à organização *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○

CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B3 Mídias sociais (fóruns, chats, listas, blogs etc.) EXTERNOS à organização *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B4 Conversa com ex-colegas de cursos, capacitações (presencial ou on-line) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B5 Encontros oficiais INTERNOS à sua organização (debates, palestras, workshops etc.) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B6 Conversa com colegas da 'sua' organização/instituição *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B7 Conversa com chefes/supervisores da 'sua' organização *

	0	1	2	3	4

RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B8 Reuniões informais INTERNAS à organização *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B9 Mídias sociais (fóruns, chats, listas, blogs etc.) INTERNOS à sua organização. *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B10 Base de dados da 'sua' organização (sistemas, relatórios, políticas etc.) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B11 Publicações governamentais (normas, regulamentos, manuais etc.) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B12 Livros impressos ou eletrônicos *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B13 Revistas e artigos científicos *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B14 Anais de congressos científicos *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B15 Trabalhos/resumos de áreas afins *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B16 Mecanismos de busca na internet (google, cade e outros) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

B17 Portais EXTERNOS à organização (empresas, organizações de segurança etc.) *

	0	1	2	3	4
RELEVÂNCIA	○	○	○	○	○
CONFIABILIDADE	○	○	○	○	○
ACESSIBILIDADE	○	○	○	○	○

« Voltar Continuar »

66% concluído

Editar este formulário

Universidade de Brasília

Programa de Pós-Graduação em Ciência da Informação

Comportamento informacional dos profissionais que atuam na segurança cibernética no âmbito da APF.

*Obrigatório

3º BLOCO: USO DA INFORMAÇÃO

No desempenho das suas atividades diárias como profissional de segurança cibernética, ou seja, relacionadas a preservação da confidencialidade, da integridade e da disponibilidade da informação na internet, incluindo não somente o hardware, software e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes no seu ambiente de trabalho/Organização.

A utilização da informação deverá ser avaliada numericamente e de forma crescente de 1 (menor) a 4 (maior) de acordo com a sua Frequência e Pertinência (Apropriado, importante):

1 para pelo menos 01 vez ao ano / Não Pertinente
2 para pelo menos 01 vez ao mês / Pouco Pertinente
3 para pelo menos 01 vez na semana / Pertinente
4 para pelo menos 01 vez ao dia / Muito Pertinente

e 0 (zero) caso não utilize esse tipo de informação.

C1 Uso das informações para atividades de resposta a incidentes de segurança em redes de computadores *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C2 Uso das informações para Suporte e atendimento aos usuários *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C3 Uso das informações para atividades de resolução de problemas de hardware, software, sistemas de informação e redes da organização/instituição *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C4 Uso das informações para atividades de Aprendizado como preparação para resolver futuros problemas *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C5 Uso das informações para aprimorar a segurança da informação na organização *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C6 Uso das informações para auditoria em sistemas computacionais comprometidos *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

C7 Uso das informações para reduzir as vulnerabilidades dos sistemas computacionais e redes de computadores *

	0	1	2	3	4
FREQUÊNCIA	○	○	○	○	○
PERTINÊNCIA	○	○	○	○	○

« Voltar Enviar

100% concluído.

Nunca envie senhas em Formulários Google.

APÊNDICE B - Roteiro de Entrevista

Universidade de Brasília

Programa de Pós-Graduação em Ciência da Informação

Bom dia (entrevistado), tudo bem? Muito obrigado por participar.

Apenas lembrando que a entrevista está sendo gravada para melhor coleta e análise das informações prestadas.

Sou mestrando na Faculdade de Ciência da Informação da Universidade de Brasília, e desde já agradeço sua colaboração em participar dessa entrevista que complementa o questionário enviado mês passado. A pesquisa é sobre comportamento informacional e pretendo avaliar as necessidades, as fontes de informação, a busca e o uso da informação pelos profissionais que atuam na segurança cibernética no âmbito da Administração Pública Federal (APF).

Considero que segurança cibernética encontra-se inserida no contexto da segurança da informação e pode ser definida como: a preservação da confidencialidade, da integridade e da disponibilidade da informação na Internet, incluindo não somente o *hardware, software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes.

A entrevista está dividida em três blocos:

1º Bloco: identificação do perfil e do contexto das necessidades de informação;

2º Bloco: avaliação dos principais canais e fontes de informação;

3º Bloco: uso da informação no desempenho das suas atividades no seu ambiente de trabalho/Organização.

Vamos começar.

BLOCO A - PERFIL DO PROFISSIONAL

1. Nome

2. Primariamente, ou na maior parte do tempo, suas atividades diárias no trabalho concentram-se em:

a) coordenação, planejamento e gestão de alto nível para alcançar resultados de longo prazo, referentes à gestão de continuidade, gestão de riscos, políticas de segurança organizacionais;

b) contato direto com sistemas computacionais, de controle ou rede de computadores, visando configuração, operação;

c)Triagem, análise, tratamento e resposta a incidentes de segurança em redes de computadores?

Pode exemplificar?

3. Quais as áreas de conhecimentos ou habilidades que julga importante para a realização do seu trabalho como profissional de segurança cibernética?

BLOCO B – NECESSIDADE DE INFORMAÇÃO.

4. Como e quando você percebe que necessita de informação?

5. Essa necessidade de informação surge bem definida?

6. Quando falamos em fontes de informação para a execução do seu trabalho como profissional de segurança cibernética, quais as cinco primeiras palavras ou expressões que lhe vem à cabeça?

BLOCO C – BUSCA E USO DA INFORMAÇÃO.

7. Como inicia a sua busca?

8. O que o faz desistir?

9. Descreva o modo com você busca a informação?

10. Como você utiliza a informação na maior parte das suas atividades/tempo?

11. Você teria algo mais a acrescentar? Pode ser referente ao questionário ou à pesquisa como um todo?

Novamente, muito obrigado pela sua disponibilidade e atenção ao meu trabalho.