Universidade de Brasília – UnB
Faculdade de Ciência da Informação – FCI
Programa de Pós-Graduação em Ciência da Informação – PPGCInf

PAULO HIDEO OHTOSHI

O COMPORTAMENTO INFORMACIONAL: ESTUDO COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA INTEGRANTES DA RENASIC/COMSIC

Brasília - DF
2013

Paulo Hideo Ohtoshi

O COMPORTAMENTO INFORMACIONAL: ESTUDO COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA INTEGRANTES DA RENASIC/COMSIC

Dissertação apresentada à Faculdade de 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 H. C. Fernandes
Coorientador: Prof. Dr. Edgard C. Oliveira

Brasília
2013

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1009972.

Ohtoshi, Paulo Hideo.
O38c O comportamento informacional : estudo com especialistas em segurança da informação e criptografia integrantes da RENASIC/COMSIC / Paulo Hideo Ohtoshi. -- 2013.
154 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Faculdade de Ciência da Informação, Programa de Pós-Graduação em Ciência da Informação, 2013.
Inclui bibliografia.
Orientação: Jorge H. C. Fernandes ; Co-orientação: Edgard C. Oliveira.

1. Comportamento informacional. 2. Criptografia. 3. Computadores - Medidas de segurança. 4. Usuário final (Computadores). I. Fernandes, Jorge H. C. II. Oliveira, Edgard Costa. III. Título.

CDU 002:004

FOLHA DE APROVAÇÃO

Título: "O comportamento informacional: estudo com especialistas em segurança da informação e criptografia integrantes da Renasic/Comsic".

Autor (a): Paulo Hideo Ohtoshi

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: 19 de julho de 2013.

Aprovado por:

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

Prof. Dr. Márcio de Carvalho Victorino
Membro Externo (EB)

Profª. Drª Sofia Galvão Baptista
Membro Interno (UnB/PPGCINF)

Prof. Dr. Cláudio Gottschalg Duque
Suplente (UnB/PPGINF)

Dedicatória

A DEUS,

Por sempre iluminar meu caminho

A minha esposa AURÉLIA e a meus filhos
EDUARDO, FERNANDO e FILIPE

Por incentivarem a realização deste trabalho

Agradecimentos

Às colaboradoras da PPGCinf Jucilene e Martha
Pela ajuda e solicitude.

Ao meu orientador, Prof. Dr. Jorge Henrique Cabral Fernandes
Pela compreensão, paciência e pelos conhecimentos transmitidos.

Ao meu coorientador, Prof. Dr. Edgard Costa Oliveira
Pelos ensinamentos, conhecimento e incentivo.

Aos professores Sofia Galvão Baptista, Márcio de Carvalho Victorino, Murilo Bastos da Cunha, Cláudio Gottschalg Duque
Pelos conhecimentos e experiências transmitidas.

Ao Cel. Antônio Carlos Menna Barreto Monclaro
Por autorizar e incentivar a pesquisa com os integrantes da RENASIC/COMSIC

Aos colegas da RENASIC/COMSIC
Pela colaboração e apoio na realização desta pesquisa

Ao meu pai (in memoriam)
Pelas lições de vida e pelo exemplo de superação e determinação.

Ao minha mãe (in memoriam)
Pelo carinho e apoio incondicional em momentos decisivos da vida.

Aos meus colegas de trabalho, Evander, Tertuliano, Renata, Luís Antônio, Cristiano, Maickel, Rodrigo Diegues, Tiago, Dimas, Carlo Magno e Alexandre Pasiani.
Por apoiarem e incentivarem o meu trabalho

“Tudo aquilo que conseguimos realizar
foi graças à ajuda de outras pessoas.”

Walt Disney

Resumo

Esta pesquisa analisou o comportamento informacional de um grupo de pesquisadores e especialistas integrantes da Rede Nacional de Segurança da Informação e Criptografia - RENASIC, analisando as necessidades de informação, o comportamento de busca e os usos da informação. O referencial teórico foi estruturado com base nos estudos sobre comportamento informacional; que envolvem as necessidades, a busca e o uso de informação; e nas características do profissional de segurança da informação. As necessidades informacionais foram analisadas por meio da identificação das atividades realizadas por esse grupo de especialistas. O comportamento de busca foi avaliado por meio da análise da relevância, frequência e confiabilidade das principais fontes utilizadas. O comportamento de uso foi avaliado com base nas atividades desempenhadas por esses profissionais na solução dos problemas, no aprendizado, no compartilhamento e armazenamento para uso posterior. Foram entrevistados 11 profissionais e analisados os questionários respondidos por 50 especialistas em segurança da informação que atuam nas áreas de desenvolvimento de software e hardware, segurança de redes, criptografia e de gestão da segurança da informação. Os resultados indicam que as principais fontes de informação são do tipo interna e pessoal, destacando-se a consulta aos colegas e outros especialistas; os sites especializados e os fóruns e listas de discussão. Os principais usos da informação incluem a solução de problemas e o aprendizado.

Palavras-chave: Comportamento Informacional, Criptografia, Estudos de Usuários, Gestão de Segurança da Informação, Segurança da informação.

Abstract

This research analyzes the information behavior of a group of researchers and experts in information security and cryptography that make up the National Network for Information Security and Cryptography – RENASIC, analyzing the information needs, the seeking behavior and the use of information. The theoretical framework was structured on the basis of studies on the information behavior, which involves the information needs, search and use, and the characteristics of the information security professional. The information needs were analyzed by identifying the activities performed by this group of experts. The search behavior was assessed by analyzing the relevance, reliability and frequency of the main sources used. The usage behavior was evaluated based on the activities performed by these professionals in problem solving, learning, sharing and storing for later use. Eleven professionals were interviewed and questionnaires answered by 50 experts in information security were analyzed; such experts work in the areas of hardware and software development, network security, encryption and management of information security. The results indicate that the main types of sources of information are the internal staff, emphasizing consultation with colleagues and other experts, specialized sites and forums and mailing lists. The main uses of the information include problem solving and learning.

Keywords: Informational Behavior, Cryptography, User Studies, Information Security Management, Information Security

Sumário

Lista de Acrônimos

ASIC – Application Specific Integrated Circuit

ASK – Anomalous State of Knowledge

ABNT – Associação Brasileira de Normas Técnicas

COBIT – Control Objectives for Information and Related Technology

CISA – Certified Information Systems Auditor

CPE – Common Platform Enumeration

CVE – Common Vulnerability and Exposures

CVSS – Common Vulnerability Scoring System

CWE - Common Weakness Enumeration

FIPS– Federal Information Processing Standards

FPGA – Field-programmable Gate Array

ISACA – Information Systems Audit and Control Association

ISO – International Standards Organization

ITIL – Information Technology Infrastructure Library

NIST – National Institute of Standards and Technology

NVD – National Vulnerability Database

SOC – System On-a-Chip

Lista de Figuras

Lista de Tabelas

1 Introdução

1.1 Contextualização

Na sociedade contemporânea, a informação tornou-se a principal riqueza das organizações e um ativo indispensável no desempenho de qualquer atividade. Ela está inserida em todos os ambientes e se faz presente em todas as atividades humanas, sociais, científicas, tecnológicas, culturais, políticas e econômicas.

Silva e Tomaél (2007) consideram que as pessoas e as organizações dependem da informação para seus processos decisórios e que nada poderia funcionar sem quantidade significativa de informação como elemento que impulsiona os fenômenos sociais. Sem informação não existe conhecimento, compartilhamento de conhecimento e crescimento corporativo.

Na qualidade de matéria-prima desse novo modelo capitalista, a informação se impõe como condição determinante para o desenvolvimento econômico e cultural da sociedade. Decorre desse contexto, o uso intensivo da tecnologia da informação, como mecanismo facilitador da coleta, produção, processamento, transmissão e armazenamento, que acarreta avassaladoras mudanças no mundo (VIEIRA, 2007, p.177)

O uso intensivo da tecnologia da informação e o surgimento da Internet no final do Século XX fizeram crescer o número de incidentes de segurança computacional, conforme mostram os dados da Figura 1.1.

Antes do advento da Internet, o impacto causado pelas falhas detectadas em programas de computador ficava restrito aos centros de processamento de dados e o acesso a recursos computacionais ficava limitado a um número reduzido de especialistas. Hoje, com a imensa quantidade de máquinas interligadas em rede e com o fácil acesso a esses recursos, um agente de ameaça pode explorar essa falha de qualquer lugar do mundo e o impacto causado pela exploração dessa vulnerabilidade pode gerar problemas de grandes proporções, tais como os

causados pelo ataque a infraestruturas críticas de um país, como usinas atômicas e redes de distribuição de água e energia elétrica.

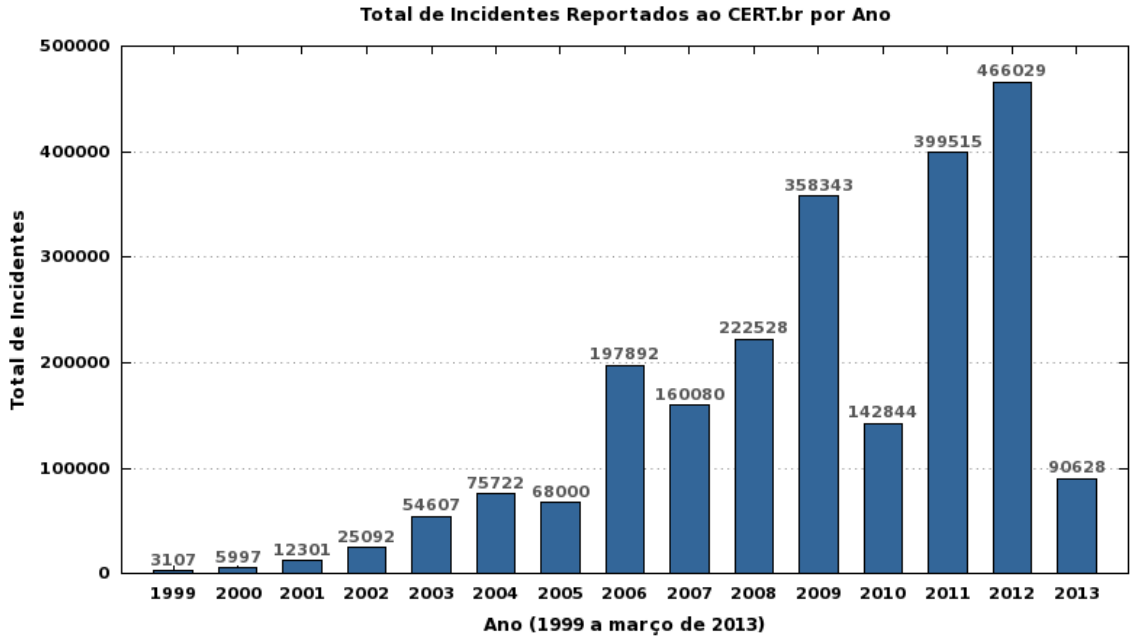

Figura 1.1 - Crescimento dos Incidentes de Segurança

Fonte: CERT.br (2013)

Diante dessas ameaças, cresce a importância da proteção dos sistemas de informação como meio de garantir a segurança dessa informação. A segurança da informação pode ser definida como a área do conhecimento dedicada à proteção de ativos de informação de forma a evitar acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003). Trata-se da área responsável por assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações. Por disponibilidade entende-se a possibilidade de acesso e utilização oportunos de informações por indivíduos e sistemas autorizados. Integridade significa que a informação não foi modificada, inclusive quanto à origem e ao destino. Autenticidade quer dizer que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo ou sistema. Confidencialidade significa acesso e divulgação restritos, ou seja, sigilo. (VIEIRA, 2007, p.180).

Nesse contexto, o profissional de segurança da informação tem um papel fundamental. Ele é o responsável pela manutenção de sistemas, pela elaboração de políticas, planos e instalação de produtos e equipamentos que protegem os ativos de informação e os dados de uma organização. Existem também profissionais que atuam na disseminação da cultura de segurança, no desenvolvimento de produtos, na análise de códigos maliciosos e em diversas outras áreas ligadas à segurança da informação.

1.2 Descrição do Problema

Hoje, manter a segurança da informação é um trabalho que pode exigir do especialista a busca em diversas fontes de informação. A tomada de decisão depende da correlação de informações que podem estar distribuídas nessas várias fontes. Processar essa informação é uma tarefa que muitas vezes pode exigir o apoio de outros especialistas, demandar tempo e ser crucial para a continuidade dos negócios.

O grande desafio desse profissional é lidar com um volume imenso de informações sobre criptografia, políticas, normas e metodologias, ameaças, vulnerabilidades, técnicas de ataque, formas de controle, normalmente dispersas em diversas fontes de informação. Esses profissionais estão submetidos a problemas já conhecidos, cujas soluções já estão armazenadas em sistemas de informação, tais como bancos de dados ou wikis[1] da organização, por meio dos quais é possível o compartilhamento de informações, ou nas anotações e registros pessoais. Há também problemas novos que exigirão a busca de novos conhecimentos e novas informações para se identificar a melhor maneira de resolvê-los.

[1] Wiki – identifica uma coleção de documentos na forma de hipertexto ou o software colaborativo usado para cria-lo.

Em ambos os casos, é desejável que o conhecimento adquirido nas pesquisas seja armazenado e compartilhado com os demais colegas, seja por meio do uso de sistemas de informação ou pela disseminação em seminários e cursos internos ou pela simples conversa diária com os colegas. Esse compartilhamento contribui para a elevação no nível geral de conhecimento, aumenta a eficiência na solução de problemas e melhora o desempenho da organização.

No desempenho de suas funções, esses profissionais buscam informações em diferentes fontes e usam a informação de diferentes formas. O estudo de comportamento informacional realizado nesta pesquisa permite estabelecer o perfil desse profissional e compreender como ele busca e usa a informação na realização do seu trabalho diário, além identificar os fatores situacionais, emocionais e afetivos que afetam esse comportamento.

Para Casado (1994), os estudos de comportamento informacional servem para: conhecer os hábitos e as necessidades de informação dos usuários; avaliar os recursos das unidades de informação, medir a eficácia das unidades de informação, adequar os espaços; conhecer a estrutura e a dinâmica de grupos de pesquisadores; conhecer as necessidades da comunidade científica. Segundo Teruel (2005), os resultados alcançados pelos estudos de usuários permitem o planejamento e o melhoramento dos serviços das unidades de informação.

Em uma área de conhecimento em permanente desenvolvimento, em que a evolução tecnológica e a inovação são as principais características, esses profissionais estão constantemente submetidos a uma demanda por atualização tecnológica. Boa parte do conhecimento necessário a essa atualização é adquirida em congressos internacionais, em que pesquisadores de todo o mundo apresentam suas pesquisas mais recentes. A participação em congressos também permite o contato direto com outros pesquisadores, por meio do qual é possível esclarecer dúvidas e solucionar problemas.

Ao abordar questões relativas às necessidades informacionais, ao comportamento de busca e ao uso dessas informações, esta pesquisa insere-se na temática da Ciência da Informação, conforme a definição de Saracevic (1996),

segundo o qual a “Ciência da Informação é um campo dedicado às questões científicas e à prática profissional, ambas voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação”.

Esta pesquisa analisou o comportamento informacional de um grupo de especialistas em segurança da informação, formado por profissionais integrantes do RENASIC[2]/COMSIC[3]. O estudo visou à identificação das fontes de informação mais utilizadas pelos especialistas em segurança da informação e dos fatores que podem influenciar a busca de informação para suprir as necessidades de informação relacionadas à atuação desses profissionais.

A pesquisa fundamenta-se na hipótese de que compreender o comportamento informacional desse grupo de especialistas em segurança da informação, a forma como buscam a informação, que fontes são as mais consultadas e que uso fazem da informação encontrada pode contribuir para aprimoramento dos processos decisórios envolvidos no exercício diário desses profissionais e para a melhoria dos processos de busca e uso da informação.

As demandas ou necessidades de informação emergem das atividades realizadas no cotidiano desses especialistas. Essas atividades são, por sua vez, resultantes dos papeis sociais que o usuário desempenha na vida. Estudar como surgem essas necessidades, como ocorrem as buscas, quais fatores cognitivos, afetivos e situacionais influenciam o comportamento de busca e como é utilizada a informação encontrada, pode auxiliar o desenvolvimento de sistemas de informação mais bem adaptados às necessidades desse profissional.

[2] RENASIC – Rede Nacional de Segurança da Informação e Criptografia

[3] COMSIC – Comunidade de Segurança da Informação e Criptografia

Para o alcance dos objetivos da pesquisa foram utilizados os fundamentos teóricos da ciência da informação e da ciência da computação, principalmente aqueles relacionados com o comportamento informacional e com a segurança da informação e criptografia, elementos essenciais na compreensão dos problemas referentes ao comportamento de busca e uso da informação dos profissionais da segurança da informação.

1.3 Questão de Pesquisa

A presente pesquisa pretende responder às seguintes questões:

1) Existe um comportamento informacional comum entre profissionais de segurança da informação?

2) Esse comportamento pode ser diagnosticado?

3) Que bases teóricas podem ser usadas?

4) Que recomendações podem ser extraídas disso para auxiliar na oferta de serviços de informação para esses profissionais?

1.4 Objetivo Geral

O objetivo geral deste trabalho é caracterizar o comportamento informacional dos especialistas em segurança da informação e criptografia, ou seja, como buscam e usam a informação sobre segurança.

1.5 Objetivos Específicos

São objetivos específicos do trabalho:

Propor um modelo teórico e um procedimento metodológico para o estudo do Comportamento Informacional do Profissional de Segurança da Informação.

Diagnosticar o comportamento informacional do profissional de segurança da informação a partir do referencial teórico

Propor recomendações para a melhoria do processo de busca e uso da informação.

1.6 Justificativa

A pesquisa propõe-se a realizar um estudo de comportamento informacional, focalizando as necessidades, a busca e o uso da informação dos especialistas em segurança da informação examinados dentro de seu contexto profissional e organizacional.

Na visão de Dias (2006, p.5), conhecer o comportamento dos usuários da informação e sua necessidade informacional é imprescindível para planejar, desenvolver e prestar serviços que, de fato, atendam as necessidades dos usuários, consumidores e produtores de informação. Assim, conhecer as necessidades informacionais do público-alvo a quem se destina determinado sistema de informação deve ser o ponto de partida no planejamento desse sistema.

Há uma carência de pesquisas sobre comportamento informacional dos profissionais que lidam com a segurança da informação. Os resultados obtidos com este trabalho podem contribuir para o aprimoramento dos sistemas de gestão da informação organizacional e para o planejamento de cursos e programas de treinamento das organizações.

No contexto atual, a realização desse estudo é relevante porque analisa o comportamento informacional de um grupo de profissionais em segurança da informação, uma área de conhecimento que tem recebido cada vez mais atenção, dada sua crescente importância e seu valor estratégico para as organizações. O estudo pode trazer grandes contribuições para os estudos sobre fontes de informação e comportamento informacional, além de subsidiar a elaboração de programas, projetos e políticas públicas.

1.7 Organização do Trabalho

A pesquisa está organizada da seguinte forma: o Capítulo 1 contém a introdução, o problema da pesquisa, os objetivos geral e específico. O Capítulo 2 apresenta uma revisão teórica de todo conhecimento necessário para a realização da pesquisa. O Capítulo 3 trata dos métodos, instrumentos utilizados, amostra e metodologia utilizada na pesquisa, bem como do modelo teórico de investigação feito com base na revisão de literatura apresentado no Capítulo 2. O Capítulo 4 apresenta os resultados da pesquisa. O Capítulo 5 a análise de discussão dos resultados. O Capítulo 6 conclui a pesquisa, apresentando uma análise geral de todo o trabalho de pesquisa.

2 Revisão Teórico-Metodológica

O objetivo deste capítulo é apresentar a fundamentação teórica sobre as questões relacionadas com o problema da pesquisa. Para tanto, é apresentada uma revisão de literatura considerada relevante para os objetivos do estudo. Na ótica do comportamento informacional, os especialistas em segurança da informação e criptografia são entendidos como usuários da informação, na medida em que esse comportamento está condicionado por necessidades de informação para a realização de seu trabalho.

O presente capítulo aborda os principais conceitos teóricos tratados nesta pesquisa, a saber: comportamento informacional (necessidade, busca e uso da informação), segurança da informação e criptografia. Destaca a importância de se estudar os usuários da informação e seus comportamentos informacionais e mostra como o conhecimento desse comportamento pode ser fundamental na melhoria dos processos de tomada de decisão, aprendizado e solução dos problemas.

2.1 Estudos de Comportamento Informacional

Os estudos de comportamento informacional ou estudos de usuários são, conforme Figueiredo (1994, p.7), “investigações que se fazem para saber do que os usuários precisam em matéria de informação ou para saber se as necessidades de informação por parte dos usuários de uma biblioteca ou de um centro de informação estão sendo satisfeitas de maneira adequada”. Por meio destes estudos, verifica-se por que, como e para quais fins os indivíduos usam informação e quais os fatores que afetam tal uso. São pesquisas realizadas para identificar e diferenciar as características, os interesses, as necessidades e os hábitos de informação dos usuários reais e potenciais de uma unidade de informação. São caracterizados 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 (SANZ CAZADO, 1994, p.31).

Os resultados alcançados pelos estudos de usuários permitem o planejamento e o melhoramento dos serviços das unidades de informação. Para Teruel (2005),

> [...] a observação sistemática do usuário oferece uma ferramenta de grande valor para tomar decisões, tanto do ponto de vista da gestão das unidades da informação como da perspectiva do bibliotecário documentalista que dia-a-dia atende seus pedidos. (TERUEL, 2005, p. 23).

Cazado (1994) entende que as aplicações dos estudos de usuários servem para:

- **conhecer os hábitos e as necessidades de informação dos usuários:** como fonte para o planejamento da unidade de informação, voltada às necessidades e informa de acordo com a necessidade de informação das comunidades de usuários a quem ela atende;
- **avaliar os recursos das unidades de informação:** busca conhecer o grau de utilização de cada um dos recursos existentes na unidade de informação para que não sejam adquiridos documentos e nem sejam mantidos serviços não utilizados ou cuja procura inexista;
- **medir a eficácia das unidades de informação:** a partir dos Estudos de usuários, é possível determinar como estão se cumprindo os objetivos da unidade;
- **adequar o espaço:** as preferências dos usuários pelo uso de determinado espaço devem ser levadas em conta no planejamento dos ambientes da unidade de informação. Estes necessitam ser pensados de modo que possam sofrer modificações no futuro, ou seja, devem ser flexíveis;
- **conhecer as necessidades da comunidade científica próxima:** o que permite disponibilizar a informações atualizadas sobre os temas de pesquisa a ela pertinentes e evitar duplicidades nas pesquisas;
- **segmentar o mercado:** para realizar programas específicos para grupos específicos.

Os estudos de usuários podem ser considerados métodos de sondagem objetiva que abrangem os estudos das “necessidades de informação” e dos “usos da informação”. Esses estudos remontam à década de 1940 e foram iniciados para responder à explosão de informações científicas e novas tecnologias, normalmente realizados por bibliotecários ou administradores de centros de informação ou laboratórios que precisavam de dados para planejar seu serviço (WILSON, 1981; CHOO, 2006 apud MIRANDA, 2006).

Gasque e Costa (2003) destacam que o termo comportamento informacional – *information behavior* – é frequentemente usado na literatura internacional. No Brasil, o conhecimento sobre comportamento informacional geralmente é abordado sob o rótulo de “estudos de usuários”.

Wilson (1999, p. 249) define comportamento informacional como as atividades de busca, uso e transferência de informação, nas quais uma pessoa se engaja quando identifica as próprias necessidades de informação.

Os estudos do comportamento informacional humano têm recebido contribuições de diversas áreas do conhecimento como a psicologia, administração, ciências biológicas, comunicação e ciência da informação. Na ciência da informação, Wilson (1999, p. 249) define comportamento informacional como as atividades de busca, uso e transferência de informação, nas quais uma pessoa se engaja quando identifica as próprias necessidades de informação.

Para Gasque e Costa (2003), o comportamento informacional envolve os seguintes conceitos:

- necessidades de informação – um déficit de informação a ser preenchido e que pode estar relacionado com motivos psicológicos, afetivos e cognitivos;
- busca da informação – ativa e/ou passiva – o modo como as pessoas buscam informações;
- uso da informação – a maneira como as pessoas utilizam a informação;

- fatores que influenciam o comportamento informacional;
- transferência da informação – o fluxo de informações entre as pessoas;
- estudos dos métodos – identificação dos métodos mais adequados a serem aplicados nas pesquisas.

Além dos principais conceitos tratados pelos estudos de usuários em ciência da informação e de sua evolução histórica, é importante destacar as diferentes abordagens desses estudos.

2.1.1 Evolução Histórica

Os estudos de usuários remontam à década de 1940, a partir do trabalho de Bernal e Urquhart, apresentado na Conferência de Informação Científica da *Royal Society*, bem como de outros trabalhos que vieram contribuir para gerar preocupação para estudos orientados às necessidades dos usuários. Esses estudos consistiam em investigações objetivas que compreendiam a análise das necessidades e dos usos da informação (WILSON, 1981; FERREIRA, 1997; CHOO, 2006).

DÉCADA	FASES DE EVOLUÇÃO DOS ESTUDOS DE USUÁRIOS
Final da década de 1940	Os Estudos de Usuários tinham como finalidade **agilizar e aperfeiçoar serviços e produtos prestados pelas bibliotecas**. Esses estudos eram restritos à área de Ciências Exatas.
1950	Intensificam-se os estudos acerca do **uso da informação entre grupos específicos de usuários**, agora abrangendo as Ciências Aplicadas.
1960	Os Estudos de Usuários enfatizam agora o **comportamento dos usuários**; surgem estudos de fluxo da informação, canais formais e informais. Os tecnólogos e educadores começam a ser pesquisados.
1970	Os Estudos de Usuários passam a preocupar-se com mais propriedade com o **usuário e a satisfação de suas necessidades de informação**, atendendo outras áreas do conhecimento como: humanidades, ciências sociais e administrativas.
1980	Os estudos estão voltados à **avaliação de satisfação e desempenho**
1990	Os estudos estão voltados ao **comportamento informacional**, que define como as pessoas necessitam/buscam/usam a informação em diferentes contextos, incluindo espaço de trabalho e vida diária.
1ª Década do Século XXI	Os estudos estão voltados tanto para o **comportamento informacional** quanto para a **avaliação de satisfação e desempenho**, enfatizando a relação entre usuários e sistemas de informação interativos, no contexto social das TIC's.

Tabela 2.1 – Evolução dos Estudos de Usuários

Fonte: Adaptado de Ferreira (2002)

De acordo Wilson-Davis (1977), esses estudos passaram a ser identificados como estudos de usuários, referindo-se a “quem” demanda (ou necessita ou recebe) “o que”, de “alguém” e “para que”. Salienta-se que os termos “quem”, “o que”, “alguém” e “para que” referem-se, respectivamente, a usuários, informação, unidades/profissionais/sistemas de informação e finalidade/necessidade de uso da informação.

Conforme Ferreira (2002), na segunda metade do século XX, os estudos de usuários passaram por diversas fases de evolução, que são apresentadas na Tabela 2.1. Os estudos de usuários até a década de 1980 eram centrados nos sistemas da informação e na sua eficiência. A maior preocupação era o perfeito funcionamento desses sistemas e de seus mecanismos de recuperação da informação.

A partir da década de 1980, o surgimento de recursos destinados à automação das tarefas documentárias e o modo de perceber esse usuário em sua interação com as máquinas despertaram diferentes interpretações e reflexões. Como principal beneficiário desses sistemas, o usuário deveria ser o centro das atenções. Começam a surgir pesquisas dedicadas especificamente ao exame daqueles que eram de fato os atores centrais de qualquer sistema de informação: não mais os aparelhos ou os artefatos, mas os usuários (FIGUEIREDO, 1994).

A Tabela 2.2 mostra o crescimento dos estudos de usuários no período de 1970 até 2007.

Período	Número de Referências	Média por Década
1970-1979	754	75,4
1980-1989	1088	108,8
1990-1999	1816	181,6
2000-junho/2007	**3570**	**510,0**
Total	**7.228**	

Tabela 2.2 – Crescimento da Literatura sobre Estudos de Usuários

Fonte: BAPTISTA; CUNHA (2007)

Os estudos de usuários têm sido objeto de diversas pesquisas, como mostram os estudos de Baptista e Cunha (2007, p. 169-170). Conforme esses

estudos, o crescimento da literatura sobre o assunto foi de 500 %, no período de 1970 a 2007. Nesta pesquisa, os autores pesquisaram o termo "*users*" e alguns termos relacionados como "*user survey*" e "*user needs*" e recuperaram 7.228 referências. Destas, 754 datavam do período de 1970 a 1979, 1088 de 1980 a 1989, 1816 de 1990 a 1999 e 3.570 de 2000 a 2007. Em média, foram identificados 75,4 trabalhos por ano na década de 1970, 108,8 na década de 1980, 181,6 na década de 1990 e 510, no período entre 2000 e 2007.

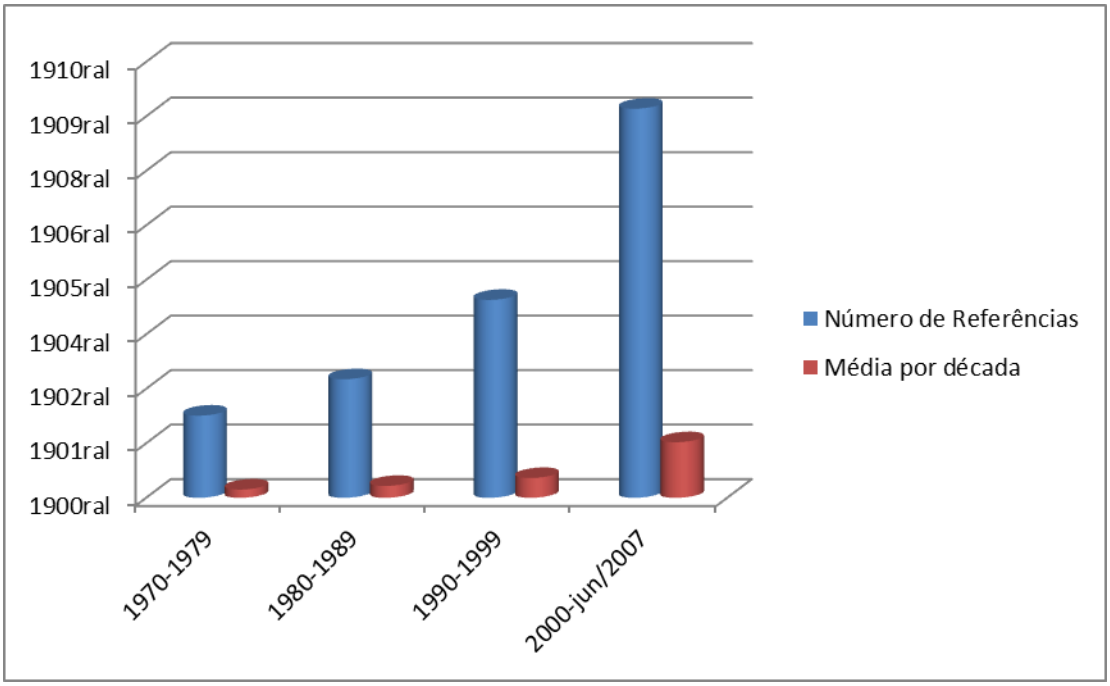

Figura 2.1 - Crescimento da Literatura sobre Estudos de Usuários

Fonte: Adaptado de Baptista; Cunha (2007)

A Figura 2.1 apresenta o crescimento da literatura sobre estudos de usuários nas últimas quatro décadas, conforme mostra o gráfico da pesquisa de Baptista e Cunha (2007, p. 169-170). Observa-se, pela figura, um forte crescimento do número pesquisas sobre estudos de usuários na última década.

2.1.2 Abordagens dos Estudos de Usuários

Os estudos de usuários tiveram o foco e a orientação ampliados ao longo dos anos na ciência da informação, passando de uma orientação centrada em sistemas para uma orientação centrada no usuário. Dervin e Nilan (1986) apud Miranda

(2006) concluíram que era necessário mudar o foco e deixar de lado o paradigma tradicional e desenvolver uma forma alternativa para os estudos de necessidades e usos de informação.

Foram detectados novos direcionamentos, apontando para as seguintes tendências:

- as necessidades dos usuários deveriam se tornar o foco central da operação de sistemas;
- os serviços de informação deveriam ser ajustados às necessidades específicas do indivíduo, e não o contrário;
- deveria ser mudado o foco dos sistemas de informação dirigidos a tecnologias e conteúdos para os dirigidos aos usuários;
- deveria ser colocado o foco nos próprios usuários.

A tipologia dos estudos de comportamento informacional proposta por Wilson-Davis considera os dois grandes grupos de estudos em matéria de pesquisas com usuários da informação. Ferreira (2002, p.7) e Figueiredo (1978, p.80) também tratam dessa temática com bastante propriedade. Na realidade, trata-se de duas abordagens aplicadas aos estudos de usuários:

- **Abordagem tradicional** – estudos direcionados sob a ótica do sistema de informação ou biblioteca (*system-oriented approach ou traditional approach*) e;
- **Abordagem alternativa** – estudos dirigidos direcionados sob a ótica do usuário (*user-oriented approach ou alternative approach*).

A Tabela 2.3 apresenta uma comparação entre os conceitos de “informação” e “necessidade de informação” na pesquisa tradicional e na alternativa:

	PESQUISA TRADICIONAL	PESQUISA ALTERNATIVA
Informação	Propriedade da matéria, mensagem, documento ou recurso informacional, qualquer material simbólico publicamente disponível.	O que é capaz de transformar estrutura de imagens, estímulo que altera a estrutura cognitiva do receptor.
Necessidade de Informação	Estado de necessidade de algo que o pesquisador chama de informação, focada no que o sistema possui e não no que o usuário precisa.	Quando a pessoa reconhece que existe algo errado em seu estado de conhecimento e deseja resolver essa anomalia, estado de conhecimento abaixo do necessário, estado de conhecimento insuficiente para lidar com a incerteza, conflito e lacunas em uma área de estudo ou trabalho.

Tabela 2.3 – Comparação entre a Pesquisa Tradicional e a Alternativa
Fonte: Miranda (2006, p.100)

Na **abordagem tradicional**, a informação é considerada algo objetivo, existente fora das pessoas e passível de ser transferida de uma para outra. Para Figueiredo (1994), parece ser possível que a eficiência e o sucesso das operações de um sistema possam ser medidos em função do número de fontes de informação recuperadas pelo sistema em comparação com o que foi realmente de interesse do usuário.

Na **abordagem alternativa** ou perceptiva, a informação é vista como algo construído pelo indivíduo e que só tem sentido quando integrada a um contexto. O indivíduo é visto como um ser com conhecimento, influenciado por crenças e valores, com necessidades cognitivas, afetivas e fisiológicas próprias, inserido em um ambiente com restrições socioculturais, políticas e econômicas. As necessidades, esquemas de conhecimento e seu ambiente formam a base do contexto do comportamento de busca e uso da informação, no qual os aspectos relativos à comunicação, como questionar, planejar, interpretar, criar, resolver e responder são valorizados (DERVIN, 1989).

2.1.3 Abordagem Tradicional ou Centrada no Sistema

Estudos centrados no sistema são aqueles nos quais existe a “premissa de que as necessidades de informação podem ser expressas ou reformuladas em questões, de acordo com a linguagem do sistema” (FIGUEIREDO, 1999, p.13 Apud MATTA in VALENTIM, p. 131). Nesse tipo de estudo, o usuário é visto como um ser passivo que deve se adaptar ao sistema de modo a alcançar o conteúdo informacional desejado. Entende-se que cabe ao usuário adaptar-se ao sistema, qualificando-se no entendimento do funcionamento ou lógica de busca nos sistemas.

2.1.4 Abordagem Alternativa ou Centrada no Usuário

Quanto ao paradigma centrado no usuário, Figueiredo (1999) expõe que esse paradigma preocupa-se com a individualidade de cada pessoa. Em vez de disponibilizar uma série de informações e desenvolver um método de busca de informações, pensando nos aspectos tecnológicos de um sistema ou de características puramente sociológicas dos usuários, procura-se entender qual o caminho percorrido pelas pessoas na busca pela informação. A necessidade de informação não é única, comum a todos os indivíduos, mas própria e específica de cada um deles. Procura-se dar atenção maior a entender como os usuários processam a informação do que a desenvolver o sistema em si e a inserir novas tecnologias.

Esta abordagem fundamenta-se nas seguintes ideias: i) a necessidade de informação deve ser analisada sob a perspectiva da individualidade do sujeito pesquisado, é subjetiva e única, definida no plano pessoal; ii) a informação necessária e o esforço empreendido na sua busca devem ser contextualizados na situação real de seu surgimento, isto é, devem ser considerados o tempo e o espaço de ocorrência. iii) o uso da informação deve ser determinado pelo indivíduo, cujos sentidos estão em constante construção.

Dervin e Nilan apud Miranda (2006) destacaram três abordagens como pertencentes ao novo paradigma dos estudos de necessidades e usos da informação, cujas características encontram-se na Tabela 2.4, que identifica alguns

autores que as adotaram.

Abordagem	Autores	Características da Abordagem
Valor Agregado	Taylor, MacMullin, Hall, Ford, Garvey, Mohr, Paisley, Farradane	Foco na percepção da utilidade e valor que o usuário traz para o sistema. Pretende fazer do problema do usuário o foco central, identificando diferentes classes de problemas e ligando-os aos diferentes traços que os usuários estão dispostos a valorizar quando enfrentam problemas. É um trabalho de orientação cognitiva em processamento da informação. (problema → valores cognitivos → soluções)
Construção de Sentido	Dervin, Fraser, Edelstein, Grunig, Stamm, Atrwood, Palmour, Carter, Dewdnev, Warner, Chen, Burguer, Hernon.	Conjunto de premissas conceituais e teóricas para analisar como pessoas constroem sentido nos seus mundos e como elas usam a informação e outros recursos nesse processo. Procura lacunas cognitivas e de sentido expressas em forma de questões que podem ser codificadas e generalizadas a partir de dados diretamente úteis para a prática da comunicação e informação. (situação → lacuna cognitiva e de sentido →uso)
Anomalia cognitiva	Belkin, Oddy, Ofori-Dwumfuo.	Foco nas pessoas em situações problemáticas, em visões da situação como incompletas ou limitadas de alguma forma. Usuários são vistos como tendo um estado de conhecimento anômalo, no qual é difícil falar ou mesmo reconhecer o que está errado, e enfrentam lacunas, faltas, incertezas, e incoerências, sendo incapazes de especificar o que é necessário para resolver a anomalia. (situação anômala → lacunas cognitiva → estratégias de busca)

Tabela 2.4 - Principais Abordagens Alternativas
Fonte: Dervin e Nilan (1986, p. 19-24) apud Miranda (2006, p.100).

Já na visão de Ferreira (1997, p.12) apud Miranda (2006, p.100), há quatro diferentes vertentes na abordagem alternativa. Para Ferreira, há pontos em comum entre as abordagens, uma vez que todas elas tendem a isolar o que o usuário percebe como dimensão fundamental de uma situação-problema, bem como o que pode ser expresso por diferentes estratégias cognitivas utilizadas pelos usuários, para especificarem que tipo de informação será útil a eles:

- Abordagem do Valor Agregado, de Robert Taylor (*User-Values ou Value-Added*);

- Abordagem do Estado Anômalo de Conhecimento, de Belkin e Oddy (*Anomalous States-of-Knowledge*);
- Abordagem do Processo Construtivista, de Carol Kuhlthau (*Constructive Process Approach*); e
- Abordagem da Construção de Sentido, de Brenda Dervin (*Sense-Making)*.

Para Ferreira, as três primeiras abordagens trazem contribuições conceituais e teóricas para um paradigma alternativo em estudos de usuários. Já a Abordagem *Sense-Making* vai mais além, ao apresentar um método para mapear as necessidades de informação sob o ponto de vista do usuário (FERREIRA, 1997 apud MIRANDA, 2006, p.100)

2.1.5 Comportamento Informacional

Em artigo publicado em 2000, Wilson propõe quatro definições relacionadas ao comportamento informacional (WILSON, 2000 apud GASQUE & COSTA, 2010):

- **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;
- **comportamento de busca da informação**: a atividade ou ação de buscar informação em consequência da necessidade de atingir um objetivo;
- **comportamento de pesquisa de informação**: o nível micro do comportamento, em que o indivíduo interage com sistemas de informação de todos os tipos;
- **comportamento do uso da informação**: constitui o conjunto dos atos físicos e mentais e envolve a incorporação da nova informação aos conhecimentos prévios do indivíduo.

Para Wilson (1981) apud Cruz 2011, o comportamento informacional refere-se às atividades de **busca**, **uso** e **transferência** de informação nas quais uma pessoa se engaja quando identifica as próprias necessidades de informação.

2.1.6 Necessidades de Informação

Para Wilson (1981), o conceito de necessidade informacional descreve uma experiência subjetiva que ocorre apenas na mente de cada indivíduo, não sendo, portanto, diretamente observável. A necessidade só pode ser conhecida por dedução, por meio da observação do comportamento, ou pela enunciação da pessoa que a detém essa necessidade.

A definição de Burnkrant (1976) apud Wilson (1996) já deixava evidenciado o caráter subjetivo da necessidade de informação. Segundo o autor, a necessidade de informação é uma representação cognitiva da futura conquista de um desejo.

Essa natureza subjetiva também se reflete na categorização proposta por Morgan e King (1971 apud WILSON, 1996), segundo os quais, as necessidades surgem a partir de três tipos de motivos: a) motivos fisiológicos (por exemplo: fome e sede); b) motivos de desconhecimento (por exemplo: curiosidade e estímulo sensorial); c) motivos sociais (por exemplo: desejo de aprovação, *status*).

Wilson (1981) tipifica as necessidades informacionais em cognitivas, afetivas e emocionais e assinala a existência de ”motivos” na origem dos comportamentos informacionais. Neste mesma linha, Cooper (1971 apud DERR, 1983, p.276) assinala que a necessidade informacional é um estado psicológico: “uma necessidade informacional é algo não observável diretamente”, isto é, não podemos ver suas “estruturas”, mas ela existe pelo menos na mente dos usuários.

Derr opõe-se a esse caráter psicológico da necessidade da informação. Na visão de Derr (1983), a necessidade de informação não é um estado psicológico e sim uma condição objetiva: “para o indivíduo, existe uma relação entre a informação e a finalidade dessa informação” (DERR, 1983, p. 276). Segundo Derr, a necessidade de informação reside em uma condição observável em que

determinada informação contribui para o alcance do objetivo que a gerou. Derr observou esse conceito em diversas etapas, afirmando que a falta de informação não significa obrigatoriamente uma necessidade de informação. O desejo de ter uma informação não é suficiente para dizer que há uma necessidade de informação. Por outro lado, o fato de se ter uma informação não elimina a necessidade dessa informação. Segundo Derr (1983), para que se configure a necessidade de informação, duas condições devem estar presentes: a) a existência de um propósito para a informação; b) que essa informação contribua para atingir esse propósito.

As necessidades informacionais estão relacionadas com as atividades profissionais de cada indivíduo e são influenciadas por vários fatores: a) fatores demográficos, tais como idade, profissão, especialização, estágio na carreira.

Kuhlthau (1993, p.5) explica que é possível entender a necessidade de informação como a "lacuna entre o conhecimento do usuário sobre seu problema ou tópico e o que o usuário necessita saber para resolver o problema".

Choo (2003, p.96) apud Souto (2010, p.81) considera que 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 fontes de informação. Satisfazer uma **necessidade cognitiva**, então, seria armazenar a informação que responde ao que se perguntou". Contudo alerta para o fato de que a informação também tem que satisfazer as **necessidades afetivas** (**ou emocionais)**, aqueles decorrentes de sentimentos relacionados às necessidades de informação e de como o indivíduo se reconhece dentro do próprio processo de busca da informação. Choo (2006, p 112) enfatiza que a existência das **necessidades situacionais**, ou seja, aquelas que podem surgir a partir do cotidiano das pessoas.

A percepção de necessidade de informação, segundo a abordagem de Taylor (1968) apud Choo (2006, pp. 97, 98), pode ser dividida em quatro níveis de categorias, conforme mostra a Tabela 2.5.

Choo (2003) ainda destaca que ver a necessidade de informação emergir em

múltiplos níveis evidencia o fato de que a satisfação da necessidade de informação vai muito além de encontrar informações que respondam à questão expressa nas perguntas ou tópicos descritos pelo indivíduo. A informação será considerada valiosa se satisfizer o estado visceral de intranquilidade que originou a necessidade de informação. A representação da necessidade da informação como visceral e consciente é semelhante à formulação de Belkin (1980) que considera a necessidade da informação como um estado anômalo do conhecimento, na qual o indivíduo não é capaz de expressar sua necessidade porque não consegue especificar o que ainda não sabe o que está faltando.

Nível	Descrição
Visceral	Vaga sensação de insatisfação, um vazio de conhecimento, quase sempre inexprimível em termos linguísticos. Essa necessidade torna-se mais concreta, à medida que o indivíduo obtém novas informações, a partir de então, a necessidade visceral entra no nível consciente.
Consciente	O indivíduo consegue descrever mentalmente a área de indecisão por meio de afirmações vagas e narrativas que refletem ambiguidade. Para estabelecer o foco a pessoa pode consultar colegas e amigos. Quando essa ambiguidade é reduzida, a necessidade para do nível consciente par o nível formalizado.
Formalizado	O indivíduo já é capaz de fazer uma descrição racional da necessidade de informação, expressa, por exemplo, por meio de uma pergunta ou um tópico.
Adaptado	A questão modificada ou reelaborada numa forma que possa ser compreendida ou processada pelo sistema de informação, A questão finalmente apresentada representa a necessidade de informação no nível adaptado.

Tabela 2.5 – Níveis de Necessidade de Informação (TAYLOR, 1968)

Fonte: Choo (2006, pp. 97, 98)

Para Kuhlthau apud Choo (2003), o princípio da incerteza estabelece que os sentimentos de insegurança e de incerteza predominam nos primeiros estágios de busca. A segurança cresce à medida que a busca prossegue e a incerteza começa a ceder quando o indivíduo é capaz de estabelecer um foco.

2.1.7 Busca da Informação

Para Marchionini (1997, p.5), a busca da informação é o processo pelo qual as pessoas intencionalmente se dedicam a mudar seu estado de conhecimento e para isto procuram representações físicas.

Trata-se de uma atividade social por meio da qual a informação torna-se útil para um indivíduo ou grupo. Cada indivíduo busca a informação de maneira diferente, dependendo do conhecimento das fontes e das experiências passadas. As pesquisas indicam a existência de sequências aplicáveis ao comportamento de busca. Duas pesquisas sobre o comportamento de busca se destacam: o de David Ellis e de Carol Kuhlthau.

O modelo de Choo (1999) define busca de informação como um processo pelo qual intencionalmente se procura por mensagens, documentos, dados pela identificação, seleção e interação com as fontes. Choo analisa o comportamento de busca de informação a partir de três dimensões: cognitiva, afetiva e situacional.

Na dimensão cognitiva são estabelecidos critérios para a seleção da informação, como **utilidade**, **precisão**, **relevância** e **confiabilidade**. Nesta pesquisa, os dois últimos (**relevância** e **confiabilidade**) foram adotados para a avalição da qualidade da fonte de informação. A qualidade da informação é a adequação a padrões estabelecidos pela necessidade do consumidor da informação (CHOO, 2000 apud NADAES, 2010, p. 207).

Segundo Choo (2003), a dimensão cognitiva é analisada do ponto de vista das características da informação por Zmud (1978), Saracevic (1970) e por Eisenberg e Schamber (1998). Zmud identifica as seguintes características: quantidade (completa ou suficiente); **confiabilidade** (verdadeira; acurada); oportunidade e qualidade no formato. Saracevic centra-se no conceito de **relevância**.

Outra pesquisa que merece destaque é aquela realizada por Saracevic et al. apud Choo (2006, p. 73). O modelo de **busca** e **armazenamento** proposto por Saracevic foi elaborado em sete principais etapas (com duas classes de variáveis entre parêntesis):

- O usuário tem um **problema a resolver** (característica do usuário, declaração do problema).

- O usuário procura resolver o problema formulando uma pergunta e iniciando uma interação com um sistema de informação (declaração da pergunta, características da pergunta).

- Interação de preinvestigação com um pesquisador intermediário, humano ou computador (característica do pesquisador, análise da pergunta).

- Formulação de uma busca (estratégia de busca, característica da busca).

- Atividade de busca e interações (busca).

- Entrega de respostas ao usuário (itens armazenados, formatos despachados).

- Avaliação das respostas pelo usuário (**relevância**, **utilidade**).

Eisenberg e Schamber (1998) apud Nadaes (2010, p. 207) definem relevância como indicador de importância, estabelecida pela relação entre o objeto julgado e uma estrutura de referência que o indivíduo possui. Para esses dois pesquisadores, a relevância é uma medida de utilidade entre um documento e uma questão julgada pelo sujeito. Depende do julgamento humano, da percepção e conhecimento do indivíduo e não de características inerentes ao documento ou à informação.

Quanto à dimensão afetiva, Choo (2000) refere-se ao grau de motivação e interesse pelo problema ou tópico que determina a soma de energia gasta na busca de informação.

Kulhthau (1993) sugere que a procura é um processo de construção de entendimento e de sentido. Desta forma, o resultado na busca de informação é influenciado pelo humor e pelas atitudes do sujeito em face à tarefa de busca. Esta se constitui, portanto, em uma série de escolhas únicas e pessoais, baseadas nas expectativas do usuário, sobre quais fontes de informação e estratégias serão

efetivas ou oportunas na solução dos problemas apresentados. Na visão de Kuhlthau, a busca de informação é composta de seis estágios, quais sejam: iniciação, seleção, exploração, formulação, coleção e apresentação. No decorrer da busca, caso se obtenha sucesso, crescem os níveis de interesse e motivação do usuário, e os sentimentos variam de incerteza a satisfação.

No nível situacional, Choo (2000) acredita que a busca da informação será a soma de tempo e esforço requeridos para localizar e contatar a fonte e interagir com ela de modo a extrair a informação. Muitos estudos destacam que a acessibilidade da fonte é fator predominante em sua escolha. Para Culnan (1985) apud Nadaes e Andrade (2010, p.208), a acessibilidade corresponde ao nível esperado de esforço requerido para usar uma fonte de informação particular.

2.1.8 Uso da Informação

Choo (2003) destaca que o fato de ser uma experiência cotidiana subconsciente, torna-se difícil conceituar satisfatoriamente o que é “uso da informação”. Segundo Choo (2003), o uso da informação envolve a seleção e o processamento da informação, de forma a **responder uma pergunta**, **resolver um problema**, **tomar uma decisão**, **entender uma situação**. A informação vai ser selecionada ou ignorada, dependendo de sua **relevância** para a **solução dos problemas** ou **esclarecimento de uma questão**.

Taylor (apud CHOO, 2006, p105) propõe oito categorias de uso da informação:

1) **Esclarecimento**: a informação é usada para criar um contexto ou dar um significado a uma situação.

2) **Compreensão do problema**: a informação é usada de uma maneira mais específica, para permitir a compreensão de um determinado problema.

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

4) **Factual**: a informação é usada para determinar os fatos de um fenômeno ou acontecimento.

5) **Confirmativa**: a informação é usada para verificar outra informação.

6) **Projetiva**: a informação é usada para prever o que vai acontecer no futuro.

7) **Motivacional**: a informação é usada para iniciar ou manter o envolvimento do indivíduo.

8) **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.

Choo (2006, p113) destaca que o modo como a informação é utilizada depende dos atributos físicos e sociais que especificam o ambiente de uso da informação, tais como a familiaridade com a situação e o tempo disponível para lidar com o problema.

2.1.9 Modelos de Comportamento Informacional

Segundo Cruz (2010), os modelos de comportamento informacional, em relação ao grau de completude, podem se referir a um estágio particular de aquisição da informação ou apresentar uma sequência completa de atividades mentais e físicas relacionadas. Por exemplo, alguns modelos concentram-se na fase de surgimento da necessidade informacional, caracterizada pelo reconhecimento, identificação ou verbalização do problema. Esses modelos, como o de Construção de Sentido (*Sense-Making),* de Dervin (1983), ou o de Wilson (2000), abstraem o

processo intelectual de resolução de problemas do contexto e se concentram nele. Outros modelos, como o de Fletcher e Katzer (1992) apud Cruz (2010), apresentam a resolução de problemas como ambientalmente condicionada. Alguns modelos dão uma figura estática do usuário, como o modelo de Ingwersen (1995) apud Cruz (2010), e outros apresentam o usuário em ação, progredindo da definição do problema, por meio de vários estágios do processamento da informação, interação com certos sistemas de informação até a fase do processamento e uso da informação, em geral explorando as características dinâmica e cíclica do comportamento informacional.

2.1.9.1 Modelos de T.D. Wilson

Baseado nas necessidades fisiológicas, cognitivas e afetivas dos indivíduos, Wilson (1981) criou um modelo de comportamento informacional. Nesse modelo, o contexto das necessidades é formado pelo próprio indivíduo, pelas demandas de seu papel na sociedade e pelo meio ambiente no qual sua vida e seu trabalho se desenvolvem. As barreiras que interferem na busca da informação surgiriam deste mesmo contexto (WILSON, 1981, MARTINEZ-SILVEIRA, ODDONE, 2007).

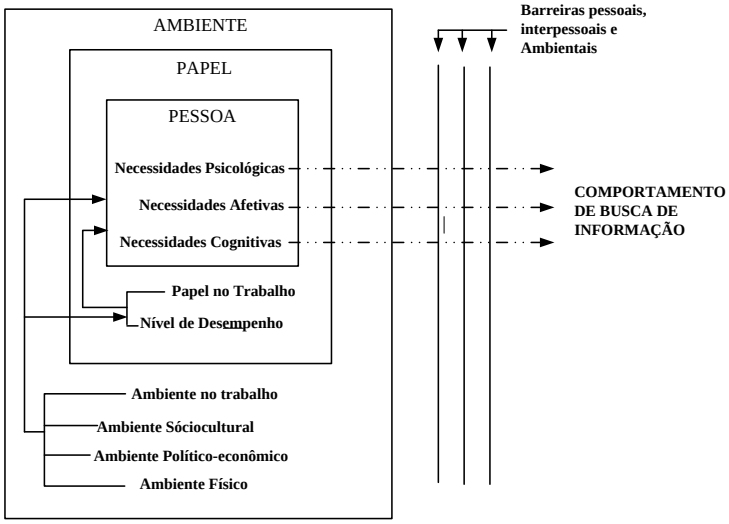

Figura 2.2 – Modelo de Necessidades e Busca da Informação de Wilson
Fonte: WILSON (1981, p. 5).

As necessidades de informação, no modelo descrito na Figura 2.2, envolvem três questões básicas. A primeira diz respeito à pessoa e envolve suas

necessidades físicas, afetivas e cognitivas. A segunda relaciona-se com o papel social que ele desempenha na sociedade; e a terceira, com o ambiente ou contexto (por exemplo: econômicos, tecnológicos e políticos), que influenciam os diferentes papéis sociais que ele exerce.

A partir da percepção da necessidade de informação, o indivíduo irá, provavelmente, engajar-se em atividades de busca da informação, nas quais poderão surgir barreiras relacionadas com as questões descritas. Nessa perspectiva, os mesmos elementos que estimulam a busca da informação, podem dificultar o processo e a maneira como o indivíduo age durante a busca da informação. Portanto, essas barreiras definem o comportamento informacional dos indivíduos.

2.1.9.2 Modelos de Dervin

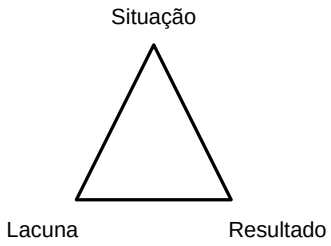

Figura 2.3 – Estrutura do Modelo de Sense-Making de Dervin
Fonte: Dervin, 1983

Em 1983, Dervin desenvolveu um modelo conhecido como *sense-making,* do qual fazem parte os seguintes elementos: (a) a situação, em tempo e espaço, seria o contexto no qual surge o problema informacional; (b) a lacuna (*gap*), que seria a distância entre a situação contextual e a situação desejada (incerteza); (c) o resultado, que representa a consequência do processo de *sense-making* (DERVIN, 1983).

Dervin (1983), empregando a metáfora do modelo de *sense-making*: situação-lacuna-resultado e exemplificou a ponte, que constitui o meio de preencher a lacuna entre a situação e o resultado, como descreve a Figura 2.4. Na visão de Dervin, toda necessidade informacional surge da descontinuidade no conhecimento provocada por uma lacuna. Em seu cotidiano, os indivíduos procuram preencher as lacunas

informacionais de diversas formas, que incluem **estudar**, **pesquisar** e **conversar** com outras pessoas. A satisfação das necessidades informacionais decorre de um acréscimo de degraus na experiência de um indivíduo. Em determinado tempo espaço, cada momento é um degrau.

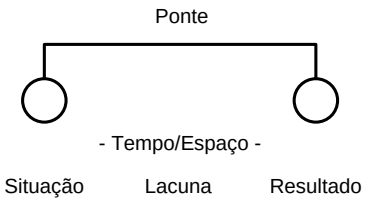

Figura 2.4 – Metáfora do Modelo de Sense-Making de Dervin
Fonte: Dervin, 1983

Cada momento em determinado tempo e espaço é um novo degrau. Os degraus relacionados à definição e ao fechamento da lacuna configuram estratégias cognitivas necessárias à obtenção de respostas, algo bastante difícil de fazer e que depende do indivíduo e da situação. Neste percurso, o indivíduo precisa de esforço para se perceber, perceber o meio ambiente e ir efetuando os ajustes necessários (DERVIN, 1983).

A importância do modelo de Dervin se reflete nas análises metodológicas que gerou, trazendo à tona questionamentos que podem revelar a natureza de uma situação problemática, podem indicar até que ponto a informação serve de ponte entre a lacuna e a satisfação, assim como podem definir os resultados do uso da informação (WILSON, 1999).

2.1.9.3 Modelo de Ellis

Em 1989, Ellis elaborou um modelo do comportamento humano na busca informacional, conforme a Figura 2.5. Esse modelo não envolvia um diagrama, mas uma série de categorias de atividades de busca informacional: **iniciar** (atividades de início da busca); **encadear** (prosseguir a busca); **vasculhar** (busca semidirigida em locais potenciais de busca); **diferenciar** (filtrar e selecionar); **monitorar** (continuar revendo as fontes identificadas como essenciais); **extrair** (trabalhar sistematicamente com as fontes de interesse); **verificar** (conferir a veracidade das

informações) e **finalizar** (ELLIS, 1989 apud WILSON, 1999). A importância do modelo de Ellis reside no fato de resultar de pesquisa empírica e de ter sido testado em diversos estudos (WILSON, 1999). “As inter-relações ou interações entre essas categorias em qualquer padrão individual de busca informacional dependerão das circunstâncias específicas da busca em questão naquele momento particular” (ELLIS, 1989, apud WILSON, 1999).

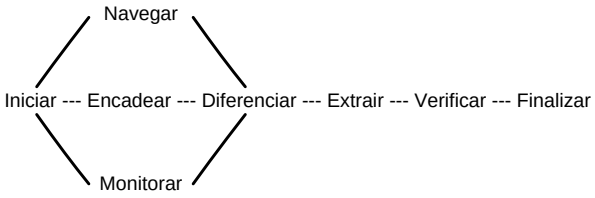

Figura 2.5 – Fase do Comportamento de Busca de Ellis
Fonte: Ellis, 1989

O modelo de Ellis pode ser aplicado no estudo do comportamento de busca na Web. Por exemplo, um indivíduo pode começar a busca em algumas páginas (iniciar); seguir alguns links para recursos relacionados (encadear); percorrer as páginas e fontes (navegar/vasculhar); selecionar como favoritas algumas fontes para futuras visitas (diferenciar); assinar serviços de alerta por correio eletrônico para receber informações (monitorar); pesquisar uma fonte específica sobre todas as informações necessitadas ou sobre um tópico em particular (extrair); verificação da precisão de uma informação (verificar); busca final por informação (finalizar) (CHOO; DETLOR; TURNBULL, 1998).

2.1.9.4 Modelos de Kuhlthau

Kuhlthau (1991) apud Choo (2006, p.87) acrescentou ao modelo de Ellis (1989) uma associação entre sentimentos, pensamentos e atitudes. Contudo, sua perspectiva é fenomenológica, não tanto cognitiva. As fases propostas por Kuhlthau são iniciação, seleção, exploração, formulação, coleta e apresentação. A iniciação, por exemplo, caracteriza-se por sentimentos de incerteza, ideias vagas sobre o tema. A atitude desta fase é simplesmente reconhecer a necessidade da informação.

Outras atitudes pertinentes são identificar, investigar, formular, coletar e completar.

Estágios	Tarefa apropriada	Sentimentos comuns e 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.

Tabela 2.6 - Processo de Busca de Informação

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

O modelo de Kuhlthau 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.

2.1.9.5 Modelo Revisado de Wilson

Em 1996, Wilson (1999) apresentou um modelo de comportamento informacional aperfeiçoado. Apesar de ter mantido a “pessoa em seu contexto” acrescentou conceitos como: os mecanismos de ativação, o caráter cíclico da busca, a importância do contexto e a categorização de variáveis intervenientes, envolvidas com os aspectos individual, social e ambiental do indivíduo. Essas características estão descritas na Figura 2.6.

O segundo modelo de Wilson (1999, p.256-257, apud CASE, p.136), baseado em outro diagrama de 1981, enfatiza o complexo contexto da busca de informação. Wilson identificou fatores neste modelo inspirado na pesquisa de outras áreas, incluindo a tomada de decisão, a psicologia, inovação, saúde, pesquisa de consumidores. Faz menção a teorias explícitas para explicar três aspectos da busca de informação:

- Por que algumas necessidades induzem ao comportamento de busca mais do que outras (teoria do estresse/enfrentamento)

- Por que algumas fontes de informação são usadas mais do que outras (teoria risco/recompensa da pesquisa sobre consumidores)

- Por que algumas pessoas perseguem um objetivo com sucesso e outras não, baseada na própria percepção de auto eficácia (teoria o aprendizado social, da psicologia)

Os mecanismos de ativação podem ser vistos como motivadores. O que motiva uma pessoa a buscar informação, como e em que medida. Esses motivadores (fatores) são afetados por seis tipos de variáveis intervenientes: predisposições psicológicas (por exemplo, tendência à curiosidade ou aversão ao risco); natureza demográfica (por exemplo, idade ou educação); fatores relacionados à sua função social (por exemplo, atuando como um gerente); variáveis ambientais (por exemplo, os recursos disponíveis), e as características das fontes (por exemplo, a acessibilidade e credibilidade) (CASE, 2002, p. 137).

Um aspecto importante do novo modelo de Wilson (1999) é reconhecer que há diferentes tipos de comportamentos de busca, tais como a atenção passiva, busca passiva, busca ativa e busca em andamento. No modelo de “processamento e uso da informação” de Wilson, a informação é avaliada quanto ao seu efeito sobre a necessidade e faz parte de um processo cíclico que pode se repetir enquanto a necessidade não for satisfeita. Para Wilson (1999), nesse novo modelo, as características pessoais do indivíduo e as características das fontes formais e informais de informação influenciam na ocorrência e no tipo de necessidade de informação, afetando a percepção das barreiras para obter-se a informação e as maneiras pelas quais as necessidades podem ser atendidas. Dessa forma, nem toda necessidade se transforma em atividade de busca, porque ocorrem os mecanismos de ativação que direcionam a pessoa a buscar informação, de acordo com a sua crença. Se existir a crença de já possui informações suficientes para decidir, não serão buscadas mais informações (Teoria do Stress). A Teoria do Risco/Recompensa no modelo refere-se à forma de se lidar com uma situação ou

resolver um problema: o custo ou o benefício percebido no processo de busca levará a pessoa a se decidir por se engajar ou não na busca efetiva pela informação. Além disso, este modelo contempla uma Teoria de Aprendizagem que, em princípio, melhora a eficácia de busca do indivíduo, ressalta que o comportamento de busca pode tomar formas variadas (Atenção Passiva, Busca Passiva, Busca Ativa e Busca em Andamento).

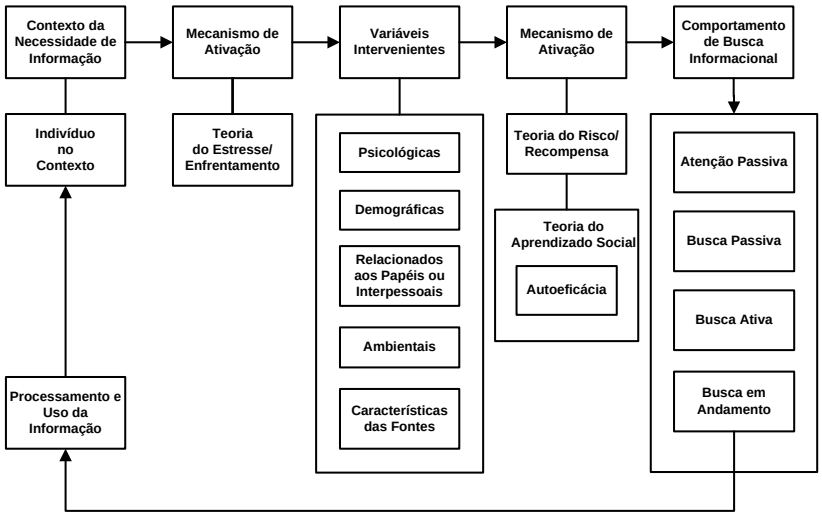

Figura 2.6 – Modelo Revisado de Wilson

Fonte: Wilson (1999)

Percebendo a existência de outra fase intermediária, agora entre a consciência da necessidade informacional e a atitude requerida para satisfazê-la, Wilson (1999) fez então uso de conceitos da Teoria do Risco/Recompensa (*Risk/Reward Theory*) para mostrar "como" e "por que", o que ele chamou de "Variáveis Intervenientes", podem desencadear ou obstruir as iniciativas de busca da informação. As fontes, por exemplo, podem tornar-se barreiras ao processo de busca: ao investigar por que algumas fontes de informação são mais utilizadas do que outras, verifica-se que, quando há várias alternativas similares a escolher, os esforços de pesquisa são proporcionais às recompensas oferecidas por cada fonte. Outro conceito empregado por Wilson para explicar o funcionamento das "Variáveis Intervenientes" foi o de "Autoeficácia" (*Self-efficacy*), oriundo da Teoria da Cognição Social (*Social Cognitive Theory*), que, por sua vez, foi desenvolvida a partir da Teoria do Estímulo-Resposta (*Stimulus-Response Theory*). A "autoeficácia" sugere a

existência de uma crença segundo a qual qualquer indivíduo sempre pode “produzir o comportamento necessário à obtenção dos resultados por ele desejados” (BANDURA, 1977, apud WILSON, 1999, p. 257). Nesse contexto, as variáveis pessoais de natureza psicológica ou demográfica, por exemplo, acabam neutralizadas pela força da “Autoeficácia”.

Observa-se, portanto, a estreita relação entre a "Autoeficácia" e as estratégias de enfrentamento, já que a crença na própria eficiência pode afetar o modo como o indivíduo responde a uma situação de necessidade informacional, o tempo e o esforço que o usuário dedica na busca. Para Wilson e Walsh (1996), uma determinada pessoa, mesmo ciente da utilidade de uma fonte de informação, pode falhar no uso dela, se estiver insegura sobre sua capacidade de lidar corretamente com essa fonte. O comportamento descrito no modelo revisado de Wilson e Walsh (Figura 2.6) envolve maior número de elementos que o da “busca ativa”.

2.1.9.6 Modelo de Choo

Choo (1999) argumenta que a “informação” é muitas vezes descrita como um “recurso”, como alguma “coisa” que reside em documentos, sistemas de informação ou em outros artefatos. A informação é considerada como algo constante, imutável. Seu significado é estabelecido pela sua representação no artefato. Uma visão complementar é olhar para a informação não como um objeto, mas como o resultado de pessoas construindo significado de mensagens. A informação não reside em artefatos, mas nas mentes dos indivíduos. Os indivíduos criam ativamente o significado da informação por meio de seus pensamentos, ações e sentimentos. Quando os indivíduos usam a informação, a fim de resolver um problema ou executar uma tarefa, os contextos sociais da informação determinam seu valor e importância. Quando tratamos as informações como um objeto, estamos preocupados com a forma de adquirir as informações que precisamos, e como representar as informações que temos, a fim de permitir o acesso e processamento.

Quando a informação é tratada como subjetivamente construída, a preocupação reside em compreender os processos sociais e comportamentais em

que a informação é representada e empregada. Uma compreensão mais ampla do comportamento de busca de informação nos ajuda a projetar melhores processos e sistemas de informação (CHOO, 1999).

Na visão de Choo (1999), atividade de busca da informação pode ser dividida em três processos distintos: i) necessidade de informação; ii) busca da informação (efetiva); e iii) uso da informação. Cada um deles é influenciado por fatores cognitivos, afetivos, e situacionais, conforme mostra a Figura 2.7.

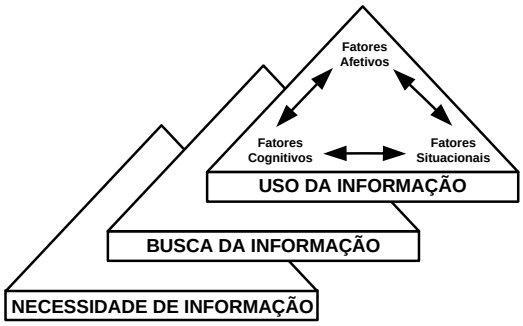

Figura 2.7 - Modelo de Choo sobre busca da informação

Fonte: CHOO (1999, p. 2).

Na camada "**necessidade de informação**", os "**fatores cognitivos**" são descritos de acordo com os princípios da construção de sentido (*Sense-Making*) de Dervin (1983). Segundo Choo (1999), a falta de sentido leva a um estado de incerteza, frustração, ansiedade e falta de confiança que, em conjunto, motivam a experiência de busca informacional. Os "**fatores afetivos**" do modelo descrevem a forma como os aspectos emocionais do indivíduo influenciam e são influenciados pela habilidade dele em construir significados para resolver as necessidades de informação. Em relação aos "**fatores situacionais**", as necessidades de informação surgem dos problemas, incertezas e ambiguidades encontradas em contextos específicos, que são compostas por uma grande quantidade de elementos, que se relacionam com as condições situacionais, tais como clareza de objetivos, consenso, magnitude do risco, quantidade de controle, normas sociais e profissionais e restrições de recursos. Choo sugere que o problema do contexto seja analisado de acordo com a dimensão dos problemas envolvidos, que ampliam as necessidades de informação e formam os critérios pelos quais os indivíduos avaliam a relevância e o valor da informação.

No modelo de Choo (Figura 2.7), a camada "**busca da informação**" relaciona-se com o processo de procura por informação por causa das necessidades de informação, como uma atitude de resolução de problemas ou como uma escolha de decisões defendida pela Psicologia Cognitiva (BEST, 1995). O indivíduo identifica as possíveis fontes, diferencia-as entre si e escolhe algumas delas para analisá-las mais de perto, para, então, obter a informação desejada. No **nível cognitivo**, o indivíduo seleciona uma fonte considerada útil, usável e relevante. A relevância e a usabilidade podem depender dos atributos da informação, tais como se a informação é abrangente, se ela é apropriada ou não para a situação específica na qual o indivíduo está envolvido. No **nível afetivo**, o grau de interesse e motivação para resolver o problema poderia determinar a quantidade de energia investida na busca informacional. No processo de busca, os sentimentos iniciais de incerteza e ansiedade se reduzem à medida que a confiança aumenta. No **nível situacional**, a seleção e o uso de fontes são influenciados pela quantidade de tempo e pelo esforço (físico, intelectual e psicológico) necessário para localizar ou contatar a fonte e para interagir com ela para extrair informação. Portanto, a seleção de fontes depende da qualidade e da acessibilidade percebida.

A camada "**uso da informação**" (Figura 2.7) está relacionada com o entendimento de uma situação particular, para saber "**o que fazer**" e "**como fazer**", para descobrir os fatos relacionados a alguma coisa, confirmar outro item de informação, projetar eventos futuros, motivar ou sustentar um envolvimento pessoal, desenvolver relações, e melhorar o status pessoal, a reputação ou a realização pessoal. No "**nível cognitivo**", o estilo e as preferências do indivíduo poderiam impactar no processamento da informação. Inúmeras classificações têm sido desenvolvidas para diferenciar tipos de personalidades e preferências cognitivas. Cada tipo de personalidade pode apresentar preferências e modos distintos de reunir e usar a informação. No "**nível afetivo**", as pessoas evitam usar informações que estimulam emoções fortes e negativas em outras pessoas ou em si mesmas. Além disso, usam a informação seletivamente para evitar conflitos ou remorsos. No "**nível situacional**", as normas e regras de um grupo social, profissão ou organização podem influenciar o processamento e o uso da informação.

Uma vez descritos os fatores **afetivos, cognitivos** e **situacionais** de cada uma das fases do comportamento informacional, Choo considera essas três fases, de forma integrada, propondo um modelo geral que representa o comportamento informacional pelos humanos (Figura 2.8).

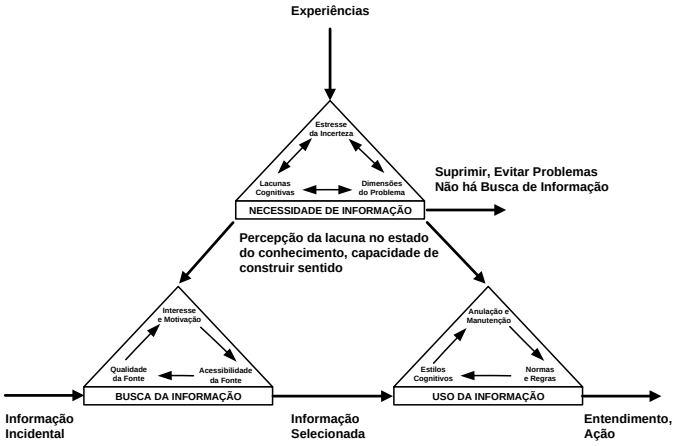

Figura 2.8 – Modelo de Comportamento Informacional Integrado de Choo.

Fonte: Choo (1999, p.6).

A percepção das necessidades de informação é marcada pelos fatores cognitivos, afetivos (emocionais) e situacionais. Nesse caso, o indivíduo pode escolher entre (i) suprimir essa necessidade e evitar a situação problemática, ou (ii) pode encará-la – partindo para um processo de busca informacional (que por sua vez também é marcada pelos mesmos fatores), ou (iii) pode decidir ignorar essa lacuna de conhecimento, partindo, diretamente, para o uso da informação (provavelmente a que ele possui em suas estruturas de memória).

Assim como existem categorias universais de necessidades de informação, Brenda Dervin e Robert Taylor apud Choo (2003) propuseram oito categorias gerais que descrevem como as pessoas usam a informação. Assim, a informação pode ser usada para: desenvolver um contexto, compreender uma situação particular, saber o que e como fazer algo, obter os fatos sobre algo; confirmar outro item de informações, projetar eventos futuros; motivar ou sustentar o envolvimento pessoal, e desenvolver relacionamentos, melhorar a reputação de status ou realização pessoal.

No nível cognitivo, o estilo cognitivo e a preferências do indivíduo teria impacto sobre o processamento de informações. Uma série de classificações foi desenvolvida para diferenciar tipos de personalidade e preferências cognitivas. O Indicador de Tipos de Myers-Briggs é um instrumento amplamente utilizado para classificar tipos de personalidade em 16 categorias. Cada tipo de personalidade mostra preferências distintas e modos sobre quando utilizar e recolher dados. Daniel Kahneman (University of British Columbia) e Amos Tversky (Universidade de Stanford) apud Choo (2003) descobriram que quando as pessoas usam a informação para fazer julgamentos elas dependem de heurísticas para simplificar o processamento de informações. Em determinadas situações, essas simplificações podem produzir erros ou preconceitos. Por exemplo, para julgar se um evento pertence a uma categoria, as pessoas confiam em estereótipos mentais e muitas vezes ignoram outras informações relevantes, tais como a distribuição das categorias da população em geral. Para julgar a frequência ou a probabilidade de um evento, as pessoas dependem de informação recente, vívida, fácil de recordar. Para estimar a quantidade fazem ajustes partindo de uma base ou ideia inicial. Infelizmente, esses ajustes são muitas vezes inadequados.

No nível afetivo, as pessoas evitam usar informações que despertem emoções fortes ou negativas nos outros ou em si mesmos. As pessoas usam as informações seletivamente para evitar o conflito, vergonha ou arrependimento, para manter a imagem e para melhorar o status ou reputação pessoal. Por exemplo, os responsáveis pela tomada de decisão são conhecidos por avaliar positivamente e continuar uma ação, mesmo quando a informação disponível indica que a retirada é necessária para reduzir as perdas. Um fator psicológico por trás dessa “escalada de compromisso” é o desejo de salvar a pele. Os tomadores de decisão persistem porque não querem admitir para si mesmos que eles cometeram um erro, muito menos expor seus erros aos outros. Em organizações em que erros na tomada de decisão são valorizados, os gestores podem tentar esconder seus erros ou adiar sua descoberta. Outro exemplo é a síndrome do "não foi inventado aqui" síndrome: a tendência de um grupo de longa data de rejeitar novas informações a partir de fora do grupo. Tal comportamento pode ser uma consequência natural de indivíduos que

ao longo do tempo tendem a aumentar a ordem e a estabilidade em seus ambientes de trabalho, de modo a reduzir a quantidade de estresse e incerteza que eles precisam enfrentar. Como resultado, mais tempo de posse dos indivíduos em um grupo, o mais forte a sua ligação emocional com crenças e decisões que ajudaram a criar, e quanto mais eles se tornam resistentes para novas ideias e informações.

No nível situacional, as normas e regras do grupo social, profissão ou organização pode influenciar o processamento e o uso de informações. Irving Janis apud Choo (2003), da Universidade Yale observou como grupos altamente coesos são suscetíveis ao “pensamento coletivo”. Isso ocorre quando os membros do grupo buscam a concordância de tal forma que comprometa o processamento e uso da informação, a escolha de ignorar ou desvalorizar informações que ameacem crenças e a solidariedade do grupo. Donald Schon do MIT descreve como cada profissão desenvolve a sua própria linguagem, valores, teorias gerais e definições de função. Os membros os adotam como base (quadros) de referência por meio da qual a informação é processada para descrever a realidade, explicar fenômenos, e reafirmar a identidade profissional. Edgar Schein da Sloan School of Management define a cultura organizacional como um padrão de pressupostos compartilhados desenvolvidos pela organização do modo como ele aprende a lidar com os problemas de adaptação externa e integração interna. Quando os pressupostos funcionam suficientemente bem, eles são considerados válidos e, portanto, ensinado aos novos membros como a maneira correta de perceber, pensar e sentir esses problemas. Como resultado, a cultura organizacional desenvolve um esquema comum de como as pessoas sentem a informação coletivamente nas organizações. Uma parte importante da cultura organizacional é política organizacional. Em uma disputa por influência e poder, a informação pode ser usada como um recurso para proteger os interesses ou para justificar os cursos preferenciais da ação.

Os três processos, necessidade de informação, busca de informação e uso de informação podem ser integrados em um único modelo geral sobre como os seres humanos buscam informação. Conforme ilustra a Figura 2.8, o indivíduo experimenta a necessidade de informação quando percebe uma lacuna em seu estado de conhecimento ou em sua capacidade de construir sentido. A percepção

da necessidade de informação é moldada por fatores cognitivos, afetivos e situacionais. O indivíduo pode escolher suprimir essa necessidade, evitando a situação problema de modo a não haver busca de informação. Como alternativa, o indivíduo pode decidir preencher esta lacuna de conhecimento ou compreensão por meio de busca de informação proposital. Durante a busca de informações, a seleção e o uso de fontes de informação dependem da acessibilidade percebida da fonte, da qualidade percebida da fonte, da complexidade da tarefa e do interesse pessoal. As informações também podem ser recebidas “por acaso”, como resultado da sondagem habitual dos meios de comunicação ou de conversas com os outros, mesmo que essas atividades não tenham sido dirigidas a atender às necessidades específicas de informação.

2.2 Segurança da Informação

Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada. A segurança da informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização (Fontes, 2006).

Segurança da Informação refere-se aos processos e metodologias que são concebidos e implementados para proteger as informações impressas, eletrônicas ou qualquer outra forma de dados privados, confidenciais, de acesso não autorizado contra o mau uso, divulgação, destruição, modificação ou interrupção.

A segurança da informação protege a confidencialidade, integridade e disponibilidade dos ativos de informação, seja no armazenamento, processamento e transmissão, por meio de políticas, educação, formação e sensibilização e technologia (Whitman & Mattfod, 2012, p.8)

Sêmola (2003, p.43) conceitua segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não

autorizados, alterações indevidas ou sua indisponibilidade".

A Instrução Normativa GSCI/PR nº 1, de 13 de junho de 2008, define Segurança da Informação e Comunicações como as ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Ainda segundo a Instrução Normativa, disponibilidade é a propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade; integridade é a propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; confidencialidade e a propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciado; autenticidade é a propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Conforme Beal (2005, p.1), "a segurança da informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade".

Para garantir a segurança da informação, é fundamental que a organização disponha de uma política de demais regulamentos para proteger a informação. A política de segurança da informação é um conjunto de diretrizes gerais destinados a governar a proteção que será dada aos ativos de informação (CARUSO e STEFFEN, 1999, p.49 apud FONTES, 2012, p.16).

A política de segurança da informação é um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações recebam a proteção conveniente que possibilite garantir a sua confidencialidade, integridade e disponibilidade (BARMAN, 2002, p.4 apud FONTES, 2012, p.16).

Essa politica ou conjunto de políticas definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados

na proteção de sua informação.

2.3 Criptografia

Com a massificação do uso da Internet e o crescimento do uso das redes de computadores pelas organizações surgiu a necessidade de se utilizar melhores mecanismos para prover a segurança das transações de informações confidenciais. A possibilidade de ter informações cruciais expostas a ameaças e a ataques cada vez mais sofisticados para violar a confidencialidade e a segurança das comunicações tornou segurança da informação um fator determinante no sucesso das organizações.

Uma das formas de se evitar o acesso indevido a informações confidenciais é codificar ou cifrar a informação de forma que somente as pessoas às quais a informação se destina sejam capazes compreendê-las. Essa técnica de codificação é conhecida como criptografia A criptografia fornece técnicas para codificar e decodificar dados, de forma a permitir que eles possam ser armazenados, transmitidos e recuperados de forma segura, ou seja, sem que sejam alterados ou expostos. Em outras palavras, as técnicas de criptografia podem ser usadas para proteger as informações suscetíveis a ataques. Elas oferecem meios de prover a comunicação segura, garantindo serviços básicos de autenticação, privacidade e integridade dos dados.

O termo criptografia, de origem grega (kryptós = “escondido” e gráphein, = “escrever”), define a arte ou ciência de escrever em cifras ou em códigos utilizando um conjunto de técnicas para tornar a mensagem incompreensível e chamada comumente de "texto cifrado", por meio de um processo chamado cifração ou encriptação, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem. As mensagens legíveis são chamadas texto claro e as codificadas, texto cifrado.

2.3.1 Criptografia Simétrica e Assimétrica

A criptografia utiliza conceitos matemáticos para a construção de seus algoritmos e pode ser usada como um meio efetivo de proteção de informações suscetíveis a ataques, estejam elas armazenadas em algum dispositivo de armazenamento de dados ou sendo transmitidas pela rede de comunicação. Seu principal objetivo é prover uma comunicação segura, garantindo serviços básicos de autenticação, privacidade e integridade dos dados.

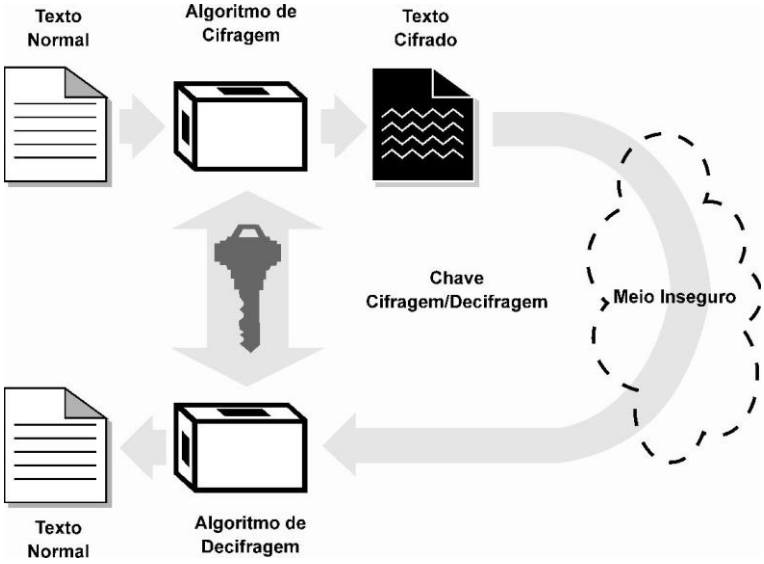

Figura 2.9 – Criptografia Simétrica

Fonte: Trinta & Macedo (1998)

A criptografia moderna classifica-se em simétrica ou assimétrica. A criptografia simétrica define uma única chave para cifrar e decifrar uma mensagem. Na criptografia assimétrica define um par de chaves, uma chave denominada pública e a outra, privada.

Na criptografia simétrica a mesma chave, compartilhada entre o emissor e o receptor, é utilizada para cifrar e decifrar a mensagem, conforme a Figura 2.9.

Em cifradores simétricos, o mesmo algoritmo usado para cifrar é usado para decifrar. Altera-se apenas a forma como as chaves são utilizadas. O texto cifrado não sofre alterações de tamanho e não contém qualquer parte da chave.

Os algoritmos de criptografia simétrica são mais rápidos do que os algoritmos assimétricos. Os algoritmos usados na criptografia simétrica, por sua vez, podem ser classificados em algoritmos em bloco e algoritmos de fluxo. A diferença entre eles está na forma como processam a informação. As cifras de fluxo processam cada bit da mensagem individualmente (processamento bit a bit), enquanto que as cifras em bloco processam blocos de informação de uma só vez, concatenando-os no final do processo. Normalmente, as cifras em bloco utilizam blocos de 64 bits ou 128 bits.

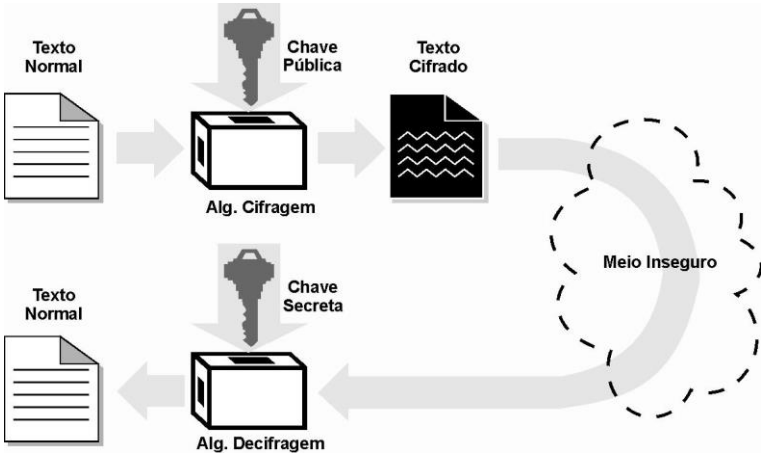

Figura 2.10 – Criptografia Assimétrica

Fonte: Trinta & Macedo (1998)

A criptografia assimétrica ou de chave pública baseia-se no uso de pares de chaves para cifrar e decifrar mensagens. As duas chaves estão relacionadas por meio de um processo matemático, usando funções unidirecionais para a codificação da informação. Uma chave, chamada chave pública, é usada para cifrar, enquanto a outra, chamada chave secreta, é usada para decifrar.

Uma mensagem cifrada com uma chave pública só pode ser decifrada pela respectiva chave secreta. A Figura 2.10 ilustra esse processo. A chave usada para cifrar recebe o nome de chave pública porque ela deve ser publicada e amplamente divulgada pelo seu detentor, fazendo com que qualquer pessoa possa lhe enviar mensagens cifradas. Já a chave usada para decifrar as mensagens, deve ser mantida em sigilo.

A revisão de literatura apresentada neste capítulo teve como objetivos subsidiar a elaboração do modelo teórico de investigação e a auxiliar a

compreensão dos principais temas tratados na pesquisa. O próximo capítulo apresenta os procedimentos metodológicos utilizados na pesquisa.

3 Procedimentos Metodológicos

Neste capítulo serão apresentados os métodos escolhidos para a obtenção de respostas às questões definida nesta pesquisa.

3.1 Método Científico

Gil (1999) define pesquisa como “o desenvolvimento do método científico de maneira formal e sistemática a fim de se obter respostas para os problemas mediante o emprego de procedimentos científicos”. Demo (1996, p.34) insere a pesquisa como atividade cotidiana considerando-a como uma atitude, um “questionamento sistemático crítico e criativo, mais a intervenção competente na realidade, ou o diálogo crítico permanente com a realidade em sentido teórico e prático”. Observando-se os conceitos definidos por Richardson (1999), constata-se que “método é o caminho ou a maneira de se chegar a determinado fim ou objetivo, e metodologia são os procedimentos e regras utilizadas por determinado método”. Conclui-se que a realização da pesquisa requer o estabelecimento claro de quais serão os procedimentos metodológicos adotados.

3.2 Classificação da Pesquisa

Quanto à natureza, a pesquisa classifica-se como aplicada, pois objetiva gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos, além de envolver verdades e interesses de um grupo definido.

Quanto aos objetivos, essa pesquisa é definida como exploratória e descritiva. Segundo Gil (1999, p.41), as pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Inclui levantamento bibliográfico e entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; análise de exemplos que estimulem a compreensão. Para o autor, a pesquisa descritiva tem como objetivo primordial a descrição das características de determinada população

ou fenômeno.

Além disso, o presente trabalho apresenta uma abordagem quantitativa, qualitativa ou mista e teórico-empírica quanto aos meios de investigação, pois exigiu o uso de métodos e técnicas estatísticas e o ambiente natural foi a fonte direta para a coleta de dados, tendo o pesquisador como o instrumento-chave.

A pesquisa adotou as abordagens quantitativa e qualitativa, considerando que essas duas abordagens seriam mais adequadas ao alcance dos objetivos traçados pela pesquisa.

Segundo Baptista e Cunha (2007), a pesquisa quantitativa aplica-se a estudos sobre a frequência de uso, acesso e para determinar características como sexo, faixa etária, ou seja, pode ser aplicada para a coleta de dados quantificáveis. As pesquisas qualitativas têm como foco a determinação de hábitos de uso e comportamento dos usuários, coletar opiniões e sugestões. Revela necessidades individuais não alcançadas pelas pesquisas quantitativas. Concentra-se nas causas das reações dos usuários e na resolução de problemas informacionais, enfatizando os aspectos subjetivos do comportamento informacional.

Esse tipo de abordagem é conhecido como abordagem mista. Segundo Morse (2003), esse método utiliza duas ou mais formas de coleta de dados em um único projeto de pesquisa. O método misto utiliza estratégias múltiplas ou mistas para responder à questão de pesquisa e testar hipóteses.

A pesquisa realizada por meio de métodos mistos, isto é, baseada em métodos quantitativos e qualitativos, produz resultados mais informativos, completos, balanceados e úteis (JOHNSON et al, 2007).

A escolha do método misto se deve ao fato de a pesquisa poder obter uma visão mais ampla e uma análise mais aprofundada do caso selecionado para a análise, obtendo informações por meio de dois caminhos diferentes e possibilitando a confrontação e validação dos resultados obtidos dessas duas formas.

3.3 Estratégia da Pesquisa

A pesquisa tem como objetivo responder às seguintes questões:

1) Se existe um comportamento informacional comum entre profissionais de segurança da informação?

2) Se esse comportamento pode ser diagnosticado?

3) Que bases teóricas podem ser usadas?

4) Quais recomendações podem ser extraídas disso para auxiliar na oferta de serviços de informação para esses professores?

Para atingir esse objetivo, esta pesquisa utilizou-se do estudo de comportamento informacional com membros da RENASIC/COMSIC, que congrega especialistas da comunidade brasileira de segurança da informação e criptografia que atuam em grandes centros de pesquisa, universidades, empresas do setor público e do setor privado e em organizações civis e militares.

Sob o ponto de vista de sua orientação, a pesquisa tem como foco o usuário, já que o objetivo é analisá-lo em seu dia-a-dia. Para Choo (2006, p. 66), a orientação para o usuário vê a informação como uma construção subjetiva, criada dentro da mente dos usuários. Em relação ao escopo, a pesquisa caracteriza-se como integrativa, uma vez que não se concentra em uma tarefa ou atividade específica, mas em todo o processo, envolvendo desde a percepção da necessidade de informação, a busca de informação, a seleção das fontes em função de sua adequação, acessibilidade e confiabilidade e, por fim, o uso dessa informação. (CHOO, 2006, p. 68). O objetivo comum neste tipo de pesquisa, na visão de Choo (2003), é identificar as fontes de informação interna e externa que são selecionadas e usadas intensivamente por grupos específicos de pessoas, ou examinar os modos formais e informais pelos quais a informação é partilhada e comunicada em profissões ou organizações definidas. As percepções e atitudes em relação à informação, à busca e as fontes de informação também são frequentemente

analisadas para determinar as preferências e padrões de uso da informação.

As pesquisas sobre comportamento informacional podem ser subdivididas em três tipos de abordagens (CASE, 2002): a) por ocupação; b) pelo papel social e; c) pelos grupos demográficos. Segundo Case (2002), a abordagem predominante é a por ocupação. Além da sua classificação segundo a abordagem, os estudos sobre comportamento informacional podem ser agrupados segundo o tipo de orientação em: a) orientados a tarefas; b) orientados a pessoas e; c) orientados a sistemas.

As pesquisas sobre o comportamento informacional de engenheiros, cientistas, cientistas sociais, pesquisadores das áreas de humanidades, ciências médicas, gerentes, jornalistas e advogados, podem ser classificados com de **abordagem ocupacional** (CASE, 2002).

Esta pesquisa caracteriza-se, portanto, como de abordagem ocupacional, uma vez que analisa um grupo de especialistas e pesquisadores pertencentes à comunidade brasileira de segurança da informação e criptografia COMSIC/RENASIC que lidam com a segurança da informação, ou seja, a pesquisa adotou uma abordagem ocupacional ou categoria profissional. Segundo Case (2002), esse é o tipo mais comum nas investigações sobre comportamento informacional e mais da metade das pesquisas é feita com esse tipo de abordagem. A pesquisa selecionou um grupo de indivíduos por sua ocupação e investigou, por meio de entrevistas e questionários, o ambiente em que atuam, sua formação acadêmica, experiência profissional e as principais atividades realizadas para poder caracterizar o contexto em que desempenham suas funções diárias. A partir dessa caracterização, foram feitas entrevistas para identificar e descrever comportamento informacional.

A abordagem foi escolhida em razão da importância do contexto nas pesquisas sobre o comportamento informacional. Segundo Dervin (1989), o contexto é tudo que não seja definido como o fenômeno de interesse. Nesta pesquisa, o ambiente, as condições de trabalho e a infraestrutura tecnológica compõem o contexto da pesquisa.

O contexto da pesquisa sobre comportamento informacional refere-se a

qualquer fator ou variável que afete o comportamento de busca dos indivíduos, tais como as condições socioeconômicas, os papéis no trabalho, tarefas, situações-problema, comunidades e organizações, incluindo suas estruturas e cultura, entre outros aspectos.

A presente pesquisa investigou as necessidades de informação por meio de três abordagens: a) identificação das categorias de problemas em que ocorrem as necessidades de informação que geram a busca de informação; b) identificação da frequência, relevância e confiabilidade das fontes de informação pesquisadas; c) identificação dos principais usos que se faz da informação obtida.

Frequência de uso das fontes, nesta pesquisa, mede a quantidade de vezes a fontes é acessada por uma unidade de tempo. Alguns estudos denominam “frequência de uso” como “audiência”. Nestes estudos, a audiência mede a disponibilidade da fonte.

Confiabilidade, de acordo com Nehmy e Paim (1998), significa credibilidade no conteúdo e na fonte da informação. Relaciona-se com a ideia de autoridade cognitiva, prestígio, respeito, reputação da fonte, autor ou instituição.

A relevância é usada “no contexto de sistemas de informação, em particular, e nos processos de comunicação em geral”, nos quais a informação “tem muitas propriedades associadas, e relevância é uma das mais importantes”. Todavia, se considerarmos que o objetivo de todo e qualquer sistema, rede ou centro de informação ou serviço é alcançar relevância nas informações oferecidas aos seus usuários, este é um problema crucial da Ciência da Informação, mesmo sabendo que a relevância será sempre relativa, ou melhor, a relevância possível (PINHEIRO, 2004).

Relevância está associada ao fornecimento de informação a tempo, regularmente, de forma efetiva e eficiente, capaz de eliminar informação não relevante, pois “se não é relevante, não é informação” e Saracevic (1996) a traduz como “uma medida de contato efetivo entre a fonte e o destinatário” e um dos seus enfoques é o de distribuições relacionadas à relevância, ou melhor, a Bibliometria

(PINHEIRO, 2004).

3.3.1 Caracterização do Estudo

O estudo feito nesta pesquisa analisou o comportamento de busca e uso da informação de um grupo de pesquisadores e especialistas em segurança da informação e criptografia integrantes da Rede Nacional de Segurança da Informação e Criptografia – RENASIC e membros da Comunidade de Segurança da Informação e Criptografia – COMSIC.

3.3.2 Abordagem Adotada

Nesta pesquisa, o método aplicado foi a triangulação por meio da obtenção de dados por vias complementares usando **questionários**, **entrevistas** e **análise documental**, conforme a definição de Creswell e Clark (2007). O modelo de triangulação adotado foi a validação de dados quantitativos. Foram utilizados questionários que foram enviados aos gestores de segurança. Esses dados foram complementados por meio de entrevistas com alguns especialistas e analisados alguns documentos referentes a grupo pesquisado.

Para Quivy e Campenhoudt (1992), o uso de questionários é uma das formas de se coletar dados em uma pesquisa. São indicados quando se investiga um fenômeno a partir da análise dos indivíduos da população em questão. Ainda segundo esses autores, as entrevistas em profundidade, que se caracterizam pelo contato direto entre o pesquisador e seus interlocutores, são usadas como método de coleta de dados quando se pretende obter informações e elementos de reflexão muito ricos e matizados. Distinguem-se pela aplicação de processos essenciais de comunicação e interação humana.

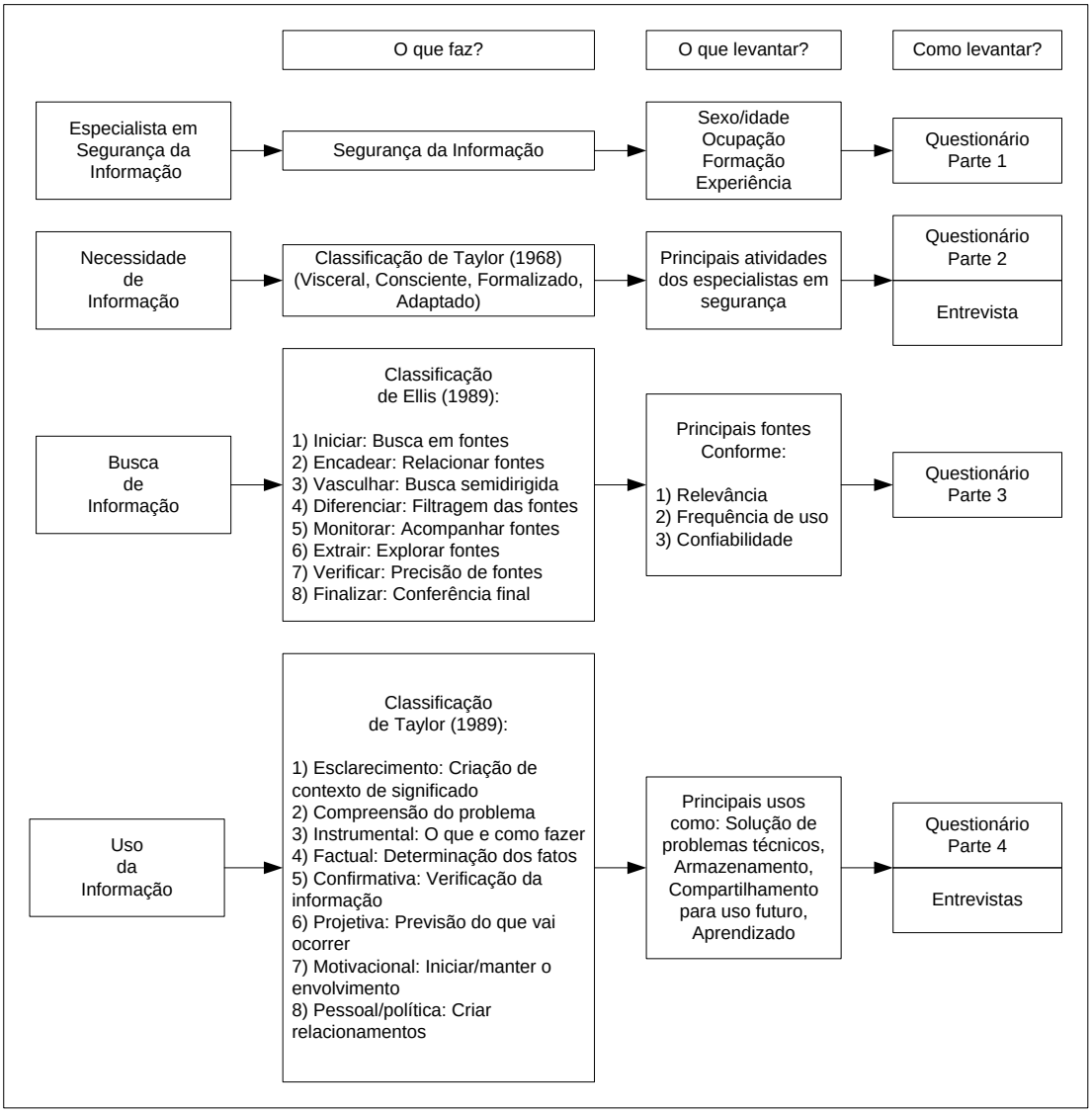

Figura 3.1 - Procedimento Metodológico da Pesquisa

Fonte: Adaptado de Choo (2003), Taylor (1968), Ellis (1989)

As informações obtidas nas entrevistas e na análise documental foram essenciais no aprofundamento da análise e na compreensão dos dados coletados por meio dos questionários. O procedimento metodológico adotado na pesquisa é apresentado na Figura 3.1.

Nesta pesquisa, baseando-se na visão desses autores, adotou-se a entrevista semiestruturada com alguns dos respondentes dos questionários, permitindo aprofundar o entendimento dos resultados coletados nos questionários. A entrevista semiestruturada utilizada nesta pesquisa é composta por perguntas abertas, feitas oralmente, seguindo uma sequência previamente estabelecida, que foram

complementadas pelo entrevistador com outras perguntas para eventuais esclarecimentos. Para complementar os dados da pesquisa qualitativa, foram realizadas pesquisas documentais para levantar alguns dados sobre o ambiente selecionado e outros aspectos relacionados ao contexto em que surgem as necessidades informacionais.

3.4 Métodos de Coleta de Dados

Definidos os objetivos da pesquisa e o modelo de análise a ser utilizado, foram elaborados os métodos por meio dos quais os dados seriam coletados. Baptista e Cunha (2007) apontam quatro métodos principais de coleta de dados: questionário, entrevista, observação e análise documental. A presente pesquisa adotou como métodos mais adequados ao estudo, a análise documental, o questionário e a entrevista. A análise documental foi utilizada na identificação do contexto, o questionário, para o levantamento dos dados sobre comportamento de busca e uso da informação e as entrevistas, para aprofundar a compreensão do comportamento dos especialistas.

Para a consecução dos objetivos da pesquisa, foram utilizados o questionário autoadministrado, as entrevistas semiestruturadas, a análise documental e a observação direta das pessoas cujo comportamento se desejava conhecer. Basicamente, procedeu-se a solicitação de informações por meio do envio de questionário a 412 profissionais atuantes na área de segurança da informação. Destes 412 especialistas, 50 participaram da pesquisa e enviaram suas respostas. Além dos questionários, foram feitas entrevistas com 11 pesquisadores e especialistas para, em seguida, mediante a tabulação e análise das respostas, obter as conclusões correspondentes aos dados coletados.

O grupo selecionado para a pesquisa é formado por pesquisadores e especialistas em segurança da informação e criptografia, que atuam em universidades, centros de pesquisa e órgãos e entidades do setor público estadual e federal e do setor privado e entidades civis e militares da RENASIC - Rede Nacional de Segurança da Informação e Criptografia. São profissionais que atuam com

segurança da informação e possuem formação superior em diversas áreas, tais como a matemática, física, engenharia elétrica, ciência da computação, engenharia de redes ou outras áreas do conhecimento.

3.4.1 Análise Documental

A análise documental permitiu identificar características importantes sobre o contexto e estrutura organizacional, bem como do trabalho realizado pelos especialistas. A estrutura organizacional está descrita em organogramas organizacionais, leis, decretos e regimentos internos. Pela análise da documentação dos projetos, tais como a especificação e o cronograma, foi possível levantar o tempo de duração e as atividades que compõem cada projeto, a quantidade de pessoas que trabalham nas atividades e os recursos necessários a sua realização.

Após o levantamento do contexto em que atuam os especialistas, foram utilizados questionários para a realização de uma pesquisa exploratória do tipo descritiva, que permitiram identificar as características do comportamento informacional desse grupo de profissionais, tendo como base os conceitos contidos no referencial teórico adotado.

3.4.2 Questionário

O questionário visou à obtenção dos dados quantitativos do comportamento informacional, ou seja, daqueles cuja análise pode ser feita por meio de gráficos, tabelas e dados estatísticos.

O questionário, composto por 21 perguntas está estruturado em quatro partes: a primeira parte visa caracterizar, por meio de oito perguntas, o perfil do pesquisado em termos demográficos (idade, sexo, área e nível de formação); a segunda parte visa identificar os temas de interesse e as atividades realizadas diariamente, por meio da qual se pretende compreender como surgem as necessidades informacionais. A terceira parte do questionário visa estudar o

comportamento de busca deste grupo de profissionais, por meio da identificação das principais fontes utilizadas e da análise da confiabilidade, frequência e relevância dessas fontes, que são dados de natureza quantitativa. Os motivos que o fazem lançar-se em busca de informação e que o fazer desistir dela foram identificados por meio de entrevistas para obtenção de informação de natureza qualitativa. A quarta e última parte do questionário é composta por um conjunto de questões com o objetivo de identificar os possíveis usos que se faz com a informação obtida.

O questionário, contendo perguntas dispostas de forma sequencial, foi elaborado com perguntas cujas respostas foram limitadas por alternativas declaradas. Elaborado em outubro de 2012 e reformulado em março de 2013, foi enviado a 412 profissionais da RENASIC/COMSIC em abril de 2013. Desses, 50 responderam ao questionário. A investigação das necessidades de informação foi feita por meio da análise das atividades realizadas diariamente por esses profissionais.

3.4.3 Entrevistas

As entrevistas semiestruturadas foram feitas com 10 representantes da categoria, selecionados conforme o papel que desempenham nas organizações em que atuam. O objetivo das entrevistas foi aprofundar e complementar os dados coletados nos questionários. Os respondentes foram selecionados entre os profissionais que atuam com o desenvolvimento de hardware e firmware criptográfico, desenvolvimento de algoritmos criptográficos, gestão de segurança de redes e gestão da segurança da informação. As entrevistas foram realizadas entre janeiro e maio de 2013

A entrevista (Anexo B) contém nove perguntas estruturadas em quatro partes: 1) Perfil do profissional; 2) Necessidade de Informação; 3) Busca de Informação; 4) Uso de Informação.

O perfil do profissional contém informações como o nome, idade, área de formação, tempo de experiência da área, tempo de experiência na organização e a as principais atividades executadas diariamente. A pesquisa parte do pressuposto

de que as necessidades emergem dessas atividades realizadas por esses especialistas.

Em relação à necessidade, a entrevista procura identificar como o especialista percebe que necessita de informação. A partir do conhecimento das atividades e das demandas de informação diárias delas decorrentes, é possível solicitar ao respondente que descreva como ele percebe que necessita de informação e se essa informação surge bem definida. Essa pergunta tem como objetivo tentar classificar a necessidade em uma das quatro categorias propostas por Taylor (1968): visceral, consciente, formalizado e adaptado.

A busca de informação é identificada pela descrição que o entrevistado faz sobre como é realizada essa busca, procurando identificar os fatores denominados por Wilson (1999) de fatores intervenientes no processo de busca e identificados como cognitivos, afetivos e situacionais, no modelo de Choo (2000). Buscou-se também caracterizar o comportamento de busca usando as fases propostas por Ellis (1989), a saber, iniciar; encadear; vasculhar; diferenciar; monitorar; extrair; verificar e finalizar (ELLIS, 1989 apud WILSON, 1999). A entrevista também procura identificar quais as fontes são usadas com frequência, quais são consideradas relevantes e quais são as mais confiáveis na visão dos especialistas.

Em relação ao uso, a entrevista pede para o respondente descrever a forma como a informação encontrada é utilizada. As possíveis categorias de uso propostas na pesquisa são: resolução de problemas, aprendizado, armazenamento, compartilhamento. Essas quatro categorias são propostas em diversos modelos e podem ser enquadradas na classificação de usos da informação proposta por Taylor (1968).

A análise dos dados obtidos por meio dos questionários foi feita mediante a tabulação dos dados da pesquisa e a criação das tabelas e gráficos. As entrevistas foram transcritas e analisadas conforme o método sugerido por Kvale (1996). O autor descreve alguns métodos para a análise e interpretação das entrevistas, entre os quais: condensação de significados, categorização dos significados, estruturação da narrativa, interpretação dos significados e geração dos significados pela

condensação das diferentes partes do material coletado nas entrevistas. Nesta pesquisa foi adotada a condensação de significados, por meio da qual a resposta fornecida pelo entrevistado é resumida em formulações breves para que, em seguida, possa ser feita a identificação dos significados das respostas.

3.5 Modelo Teórico de Pesquisa

A presente pesquisa analisou o comportamento informacional de especialistas em segurança da informação e criptografia. O modelo de análise proposto, que incluiu a discussão sobre as necessidades, o comportamento de busca e os usos de informação desse grupo de especialistas, baseou-se nos modelos propostos por Wilson (1999) e Choo (2003), incluindo os trabalhos de outros pesquisadores como Taylor (1968), Belkin (1980), Ellis (1989, 1992), Dervin (1983b, 1992) e Kuhlthau (1983, 1986, 1989).

O modelo integrativo adotado nesta pesquisa abrange todo o processo de busca e uso da informação. Entre seus objetivos, incluem-se identificar a situação e o contexto que levou ao reconhecimento da necessidade de informação, examinar as atividades de busca e o armazenamento da informação e analisar como a informação é utilizada para resolver problemas, tomar decisões e criar significado. O modelo está representado na Figura 3.2.

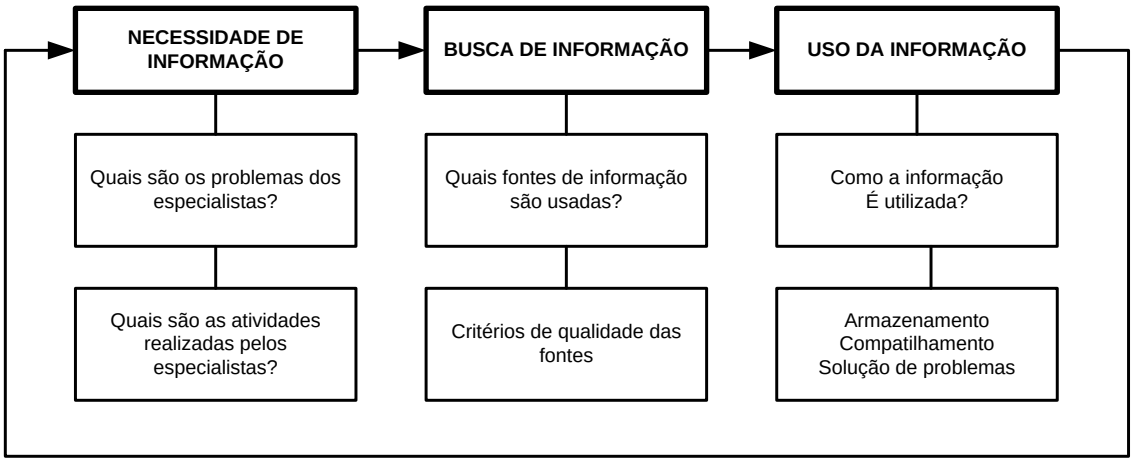

Figura 3.2 – Modelo Teórico de Pesquisa

Fonte: Baseado nos Modelos de Choo (2003), Wilson (1999) e Pereira (2008)

O modelo de Choo (2006, p.115) oferece uma estrutura para a análise do comportamento informacional ao dividir conceitualmente o processo em três estágios: necessidade, busca e uso da informação. Em cada estágio, o modelo examina os efeitos das necessidades cognitivas, reações emocionais e as demandas situacionais sobre o indivíduo.

O objetivo do modelo é auxiliar a identificação das características específicas do comportamento dos indivíduos selecionados para a pesquisa. As necessidades foram identificadas com base nas atividades realizadas pelos especialistas e pesquisadores, o comportamento de busca foi analisado com base nas fontes utilizadas e, finalmente, o uso foi analisado com base nas atividades executadas após a seleção das informações encontradas.

As necessidades, após serem percebidas pelo usuário, podem ser classificadas em quatro níveis, segundo Taylor (1968): visceral; consciente; formalizado e adaptado. No nível visceral, o indivíduo não sabe exatamente qual a sua necessidade, pode ser uma insatisfação, um vazio de conhecimento que não pode ser expressa em termos de questionamento. À medida que o indivíduo obtém novas informações, a necessidade torna-se mais clara. Quando isso ocorre, o indivíduo está no segundo nível ou nível consciente, em que o indivíduo consegue mentalmente descrever vagamente a área de indecisão ou ambiguidade. Para estabelecer um foco, a pessoa pode consultar colegas e outros especialistas. No terceiro nível, ou nível formalizado, o indivíduo é capaz de formalizar um questionamento, a ambiguidade está reduzida e o indivíduo é capaz de fazer uma descrição racional da necessidade. No quarto e último nível, ou nível adaptado, a questão formalizada é reformulada e adaptada, de forma a ser compreendida ou processada pelo sistema de informação.

No ambiente em que atuam, esses pesquisadores e especialistas enfrentam diariamente situações que geram vários tipos de necessidades. Essas necessidades variam em função do tipo de trabalho realizado e da atividade na qual o pesquisador ou especialista está envolvido.

O objetivo do modelo proposto foi possibilitar a captura das características específicas de comportamento dos indivíduos selecionados para a pesquisa em relação às necessidades, busca e uso da informação. As necessidades de informação foram identificadas com base nas atividades exercidas por esses especialistas e na análise documental, o comportamento de busca foi feito a partir da observação diretas dos especialistas e também com base no levantamento das principais fontes de informação utilizadas e, por fim, o uso da informação foi avaliado por meio da identificação das principais formas de utilização, após a seleção das informações encontradas.

Conforme o tipo de problema enfrentado pelo especialista, ele apresenta um tipo de comportamento descrito por Dervin (1983) por meio da metáfora do *Sense-making* ou de construção de sentido. Ele se depara com cada situação-problema, avalia a própria condição cognitiva para solucionar o problema e, ao perceber que há uma "lacuna" entre o conhecimento atual e o conhecimento necessário para solucionar o problema, inicia a busca de meios para alterar o seu nível de conhecimento e finalizar a sua ação.

A análise deste tipo de comportamento feita por Dervin (1983) considera a Teoria dos "Estados Anômalos do Conhecimento" (*Anomalous State of Knowledge - ASK*) proposta por Belkin (1980). Nela, o indivíduo possui uma necessidade informacional, mas não está apto a explicitar de que informação ele precisa ou qual conhecimento está faltando, o que dificulta a entrada exata de dados de busca nos sistemas de informação, a menos que esses sistemas estejam preparados para auxiliar os usuários na descrição dos problemas de forma a identificar e caracterizar as necessidades informacionais.

A partir do reconhecimento da necessidade de informação ou de que existem problemas a serem resolvidos e considerando que, do ponto de vista cognitivo, o especialista já identificou sua situação como de insuficiência de conhecimento para solucioná-lo, o que ocorre, em seguida, é o comportamento de busca de informações.

Wilson (1981) descreve a “necessidade de informação” como um processo de **tomada de decisão**, **solução de problemas** ou **alocações de recursos**. O conhecimento das necessidades de informação permite compreender por que as pessoas se envolvem num processo de busca da informação. O que levaria uma pessoa a buscar, então, informação? A existência de um problema a resolver, de um objetivo a atingir e/ou a constatação de um estado anômalo de conhecimento, insuficiente ou inadequado (Le Coadic, 1996, p. 39).

Segundo Figueiredo (1994), é importante considerar dois tipos de necessidades de informação: a necessidade de informação em função do conhecimento e a necessidade de informação em função da ação:

- A necessidade de informação em função do conhecimento é uma necessidade que resulta do desejo de saber.

- A necessidade de informação em função da ação é uma necessidade que resulta de necessidades materiais exigidas para a realização de atividades humanas, profissionais e pessoais.

A necessidade de informação em função do conhecimento surge da dúvida e do esforço de dominá-la, já a necessidade de informação em função da ação desencadeia uma ação com objetivo, visando à eficácia dessa ação. Entre essas necessidades, a informação é útil para estimular o pensamento e a ação, por meio das ideias de outras pessoas, conhecimentos, experiência e realizações; enfim, para atender as necessidades requeridas. A informação é, essencialmente, vista como um utensílio valioso e útil para o indivíduo em sua tentativa de prosseguir com sucesso sua vida (COSTA, SILVA & RAMALHO, 2009).

No modelo de comportamento informacional proposto por Wilson (1999), a busca da informação se inicia para satisfação de uma necessidade informacional, neste caso, para a solução de um problema específico ou para o aprendizado.

A partir deste momento, o usuário da informação, neste caso específico, o especialista em segurança da informação, interage com sistemas de informação

(manuais ou automatizados), consulta outros especialistas, busca a informação na literatura especializada, em resumo, toma as providências que julga necessárias para encontrar as informações que satisfaçam a necessidade de informação, seja para solucionar os problemas ou para a atualização profissional.

Finalizando o ciclo proposto por Choo (2003): necessidade, busca e uso da informação; a pesquisa analisou os principais usos que os gestores fazem da informação obtida.

Na concepção de Taylor (1968,1996), existem elementos essenciais que regem o fluxo e o uso da informação e determinam o critério por meio do qual o valor da informação vai ser avaliado. Esses elementos, que formam o contexto ou ambiente de uso da informação, podem ser reunidos em quatro categorias: i) grupo de pessoas, ii) dimensão do problema, iii) configuração do ambiente de trabalho, iv) premissas para a solução dos problemas.

4 Dados e Resultados

4.1 A RENASIC/COMSIC

Esta pesquisa analisou o comportamento de busca e uso da informação de um grupo de pesquisadores e especialistas em segurança da informação e criptografia integrantes da Rede Nacional de Segurança da Informação e Criptografia – RENASIC e membros da Comunidade de Segurança da Informação e Criptografia – COMSIC. A descrição completa da RENASIC/COMSIC é apresentada no Anexo C.

4.2 O Perfil dos Especialistas e Pesquisadores

A primeira parte da pesquisa com esse grupo de pesquisadores e especialistas que atuam em segurança da informação e criptografia objetivou coletar informações relevantes acerca do seu perfil. Esse perfil foi levantado por meio de perguntas referentes à formação, tempo de experiência e forma de atuação.

A segunda parte da pesquisa permitiu coletar informações relevantes acerca das atividades exercidas por esses profissionais em seu ambiente de trabalho. O objetivo foi identificar, por meio do mapeamento dessas atividades, as necessidades informacionais desses profissionais. A pesquisa pressupõe que as necessidades de informação surgem a partir dessas atividades.

O grupo entrevistado foi formado por especialistas que trabalham com segurança da informação ou criptografia nas seguintes áreas: 1) desenvolvimento de algoritmos e protocolos criptográficos, 2) desenvolvimento de hardware e firmware criptográfico, 3) gerenciamento de segurança de redes e, 4) gestão da segurança da informação.

4.2.1 Desenvolvimento de Algoritmos e Protocolos Criptográficos

Os profissionais que atuam no desenvolvimento de algoritmos e protocolos criptográficos elaboram soluções que envolvem o uso de criptografia. A criptografia é uma área que exige conhecimentos normalmente oferecidos por cursos de pós-graduação em matemática, estatística, engenharia ou ciência da computação. Os especialistas selecionados para esta pesquisa são profissionais com pós-doutorado, doutorado e mestrado em matemática e estatística. O dia-a-dia desses profissionais é caracterizado pelo trabalho em equipe. Cada equipe é composta por pelo menos um matemático e um estatístico que trabalham em projetos que, em média, exigem três meses a dois anos para serem concluídos. Por lidarem com tecnologias no estado da arte, buscam nos artigos publicados em revistas especializadas e nos anais de congressos internacionais e as informações de que necessitam. A criptografia estuda técnicas para garantir a confidencialidade, a integridade e a disponibilidade das informações de forma a garantir o armazenamento e a transmissão segura das informações.

Alguns algoritmos criptográficos são projetados com base na dificuldade computacional de se fatorar números grandes, o que dificulta sua quebra. Esses algoritmos são passíveis de serem quebrados na teoria, mas sua realização prática se torna inviável com os recursos computacionais disponíveis hoje.

Os sistemas elaborados com esses algoritmos são computacionalmente seguros. As melhorias nos algoritmos de fatoração de números inteiros e as tecnologias de processamento mais rápido representam avanços teóricos que exigem que as soluções sejam continuamente aperfeiçoadas.

Existem sistemas de informação teoricamente seguros, que comprovadamente não podem ser quebrados, nem mesmo com o uso de supercomputadores. Como exemplo, podemos mencionar os sistemas *one-time pad*, que são considerados extremamente seguros, mas são difíceis de serem ijmplementados e gerenciados. Os sistemas *one-time pad* utilizam chaves usadas uma única vez (“*one-time key*”). Essas chaves não podem, em nenhuma hípotese, ser reutilizadas e devem ter o mesmo tamanho da mensagem a ser criptografada.

Se o tamanho do arquivo de mensagem for de um terabyte, o tamanho da chave deverá ser de um terabyte.

Além de chaves com o mesmo tamanho da mensagem a ser criptografada, os sistemas one-time pad requerem o emprego de sequências aleatórias de boa qualidade. Com o intuito de produzir sequências aleatórias e de boa qualidade criptográfica, desenvolvem-se geradores aleatórios em *hardware*. Geradores randômicos baseados em *software* são pseudoaleatórios.

Os sistemas *one-time pad* são baseados em criptografia de chave simétrica, que apresenta, entre os principais problemas, a questão da distribuição de chaves simétricas. O número de chaves simétricas é dado pela equação N = n(n-1)/2, na qual “n” é o número de usuários do sistema e “N” o número de pares de chaves simétricas. Isso faz com que o número de chaves cresça exponencialmente com o número de usuários do sistema.

4.2.2 Desenvolvimento de Hardware e Firmware Criptográfico

O grupo de profissionais que atua como o desenvolvimento de hardware e firmware criptográfico é formado por engenheiros com graduação e pós-graduação em engenharia elétrica e por técnicos de eletrônica. O trabalho envolve o desenvolvimento de hardware específico para a aplicação em criptografia. Os projetos são desenvolvidos, em média, de um a dois anos e exigem ampla pesquisa nas fases iniciais sobre temas relativamente complexos. Uma das atividades do engenheiro de desenvolvimento é implementar em hardware ou firmware o algoritmo elaborado pelos matemáticos. Os algoritmos implementados em hardware ou firmware são notadamente reconhecidos por seu desempenho mais veloz e por sua segurança superior.

Além dessas tarefas, o engenheiro de hardware especializado em criptografia é também responsável por construir bons circuitos geradores aleatórios. Um dos desafios no projeto de geradores aleatórios é desenvolver dispositivos com capacidade de gerar sequências aleatórias de boa qualidade e em grandes quantidades. Embora sequências de bits “zeros” ou sequências de bits “uns” sejam

aleatórias, sequências muito longas de zeros ou de uns pode aumentar a vulnerabilidade, tornando o sistema quebrável e facilitar o trabalho de criptoanálise. Filtros são utilizados de modo a eliminar sequências grandes ou com padrões repetidos. O Entrevistado 11 disse que sua empresa havia desenvolvido um gerador aleatório em parceria com o Departamento de Engenharia Elétrica da Universidade de Brasília. O gerador aleatório foi desenvolvido em um circuito integrado de oito pinos utilizando a tecnologia ASIC.

Além da implementação de algoritmos criptográficos, os engenheiros projetistas trabalham com tecnologias que envolvem o processamento digital de sinais voz e imagem. O conhecimento exigido do profissional que atua nesse tipo de projeto está presente em cursos superiores de mestrado e doutorado nos campos de processamento digital de sinais, compressão de voz e de imagem, reconhecimento de padrões e criptografia. Nesse estágio de conhecimento, boa parte das informações é obtida publicações internacionais, como artigos, anais de congressos e revistas especializadas como a "*Transactions on Computers*", "*Transactions on Image Processing*" da IEEE Computer Society, que é o ramo computacional do IEEE[4]

Workshops como o CHES - *Cryptographic Hardware and Embedded Systems*, realizado anualmente em conjunto com eventos de criptografia, é um evento que trata especificamente de sistemas embarcados e hardware criptográfico, de fundamental importância para o profissional que atua na área.

[4] "*Institute of Electrical and Electronics Engineers*" - Instituto de Engenheiros Eletricistas e Eletrônicos

Figura 4.1 - Tecnologia SOC

Fonte: AMD

O uso de tecnologia como a SOC (*System on-a-Chip*), ASIC (*Application Specific Integrated Circuit*) e FPGA (*Field Programmable Gate Array Logic*), aliada ao de processadores rápidos possibilita o desenvolvimento de soluções com processamento de alto desempenho. A tecnologia SOC ou “Sistema em um Circuito Integrado”, caracteriza-se por reunir em um único circuito integrado ou “chip” vários componentes de um circuito. Essa tecnologia, utilizada em sistemas embarcados (“*embedded systems*”), permite realizar funções digitais, analógicas, incluindo a radiofrequência, todas em um único circuito integrado – CI.

Semelhante aos microcontroladores, as tecnologias SOC, em geral possuem memórias RAM internas com capacidade de até 100K de memória. Um sistema embarcado é um sistema computacional que contém partes mecânicas e elétricas embutidas em um único dispositivo. Os sistemas embarcados contêm núcleos de processamento baseados em microcontroladores ou processadores digitais de sinais (“*digital signal processors*”), executando uma tarefa ou propósito específico.

Outro tipo de recurso tecnológico muito empregado na área de criptografia é a tecnologia ASIC – *Application Specific integrated Circuit* ou circuito integrado para uma aplicação específica. Ao contrário dos circuitos integrados (CI) de uso geral, os chips com tecnologia ASIC são circuitos integrados customizados para realizar uma tarefa específica. Os primeiros circuitos integrados com tecnologia ASIC eram baseados em *gate arrays* ou uma matriz de portas ou circuitos lógicos.

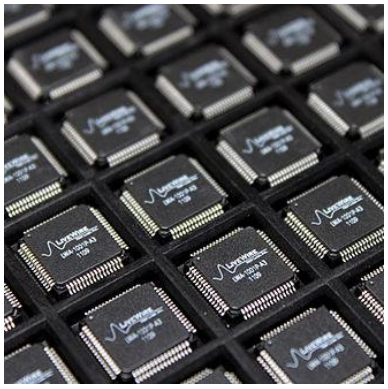

Figura 4.2 - Tecnologia ASIC

Fonte: LIVEWIRE

Os FPGA, do inglês "*Field Programmable Gate Array Logic*", ou lógica baseada em matriz de portas programável em campo, são circuitos integrados fabricados para serem reconfigurados pelo projetista. O nome "*field programmable*" designa exatamente esta característica, a de um circuito programável em campo, isto é, depois de sua fabricação. Esse tipo de tecnologia permite implementar as operações lógicas dos algoritmos criptográficos, tais como a transposição de matrizes ou o deslocamento de registros ("*shift registers"*), muito comuns nas operações contidas nas cifras de blocos e cifras de fluxo. Destaca-se o bom desempenho em termos de velocidade de processamento dos algoritmos criptográficos desenvolvidos com essa tecnologia.

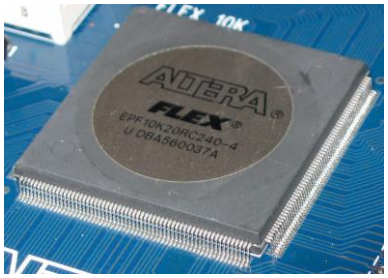

Figura 4.3 - Tecnologia FPGA

Fonte: Altera

Os dispositivos criptográficos baseados em hardware se devidamente encapsulados e protegidos tornam-se extremamente mais seguros do que os dispositivos criptográficos baseados somente em software. As normas de segurança que estabelecem as principais diretrizes para a área de desenvolvimento de

hardware e firmware criptográfico são as normas ISO/IEC 15408, conhecida como "*Common Criteria"* ou de padrões comuns e a FIPS[5] 140-2. A norma FIPS 140-2 é um padrão de segurança computacional que estabelece os requisitos de segurança para módulos criptográficos (*Security Requirements for Cryptographic Modules)* exigidos pelo Departamento de Defesa do governo americano*.*

Entre outras recomendações, a norma *Common Criteria*, estabelece critérios para evitar que os sinais eletrônicos sejam interceptados por meio da captura de sua emissão eletromagnética, mecânica ou acústica gerada não intencionalmente pelos equipamentos criptográficos. Esse efeito, conhecido como TEMPEST, codinome atribuído pela NSA (*National Securtiy Agency* - Agência de Segurança Nacional), foi utilizado pelos serviços de inteligência para interceptar as comunicações explorando os efeitos ambientais gerados por esses fenômenos associados à emanação eletromagnética, à variação do campo elétrico, à variação no consumo de energia.

Um das recomendações para evitar esse tipo de efeito são as blindagens dos cabos e das carcaças dos equipamentos. A norma também estabelece recomendações para evitar a violação dos equipamentos eletrônicos, recomendado o uso de lacres, selos, resinas e gravação de bits de segurança. Os dispositivos "*tamper proof*", ou à prova de violação, destroem seus conteúdos internos ao serem violados.

4.2.3 Gestão da Segurança da Informação

O grupo formado por profissionais que atuam na área de gestão da segurança da informação é composto por profissionais de diferentes áreas de formação, com especialização em Gestão da Segurança da Informação. O trabalho desses especialistas inclui a elaboração e a revisão periódica das políticas, normas e regulamentos internos de segurança da informação. Cabe a esses profissionais

[5] *Federal Information Processing Standard Publication* 140-2 –

zelar pelo cumprimento das normas de segurança corporativa.

A área é também responsável pelos processos de conscientização e pelos programas de treinamento feito por meio de campanhas e de cursos internos de curta duração. O processo de conscientização das pessoas é fundamental para a manutenção de um dos três pilares da segurança da informação: pessoas, processos e tecnologias.

Para adquirir e manter atualizados os conhecimentos sobre gestão da segurança da informação, além de cursos formais na área, é necessário estimular a participação dos gestores em seminários, cursos de especialização, workshops e congressos.

Os grupos de discussão, boletins e sites de organizações especializadas, disponíveis na *Internet*, também são uma boa fonte de informação (BEAL, 2008, p.21). Esses gestores devem ser encorajados a obter qualificações profissionais que testem se seus conhecimentos estão atualizados e compatíveis com os padrões profissionais internacionais.

Em alguns países existem organizações que promovem certificações de qualificação profissional por meio de cursos de preparação e exames de qualificação para obtenção de certificações ITIL[6], COBIT[7], ISO2700 e ISACA[8]. Uma das certificações recomendadas é a "*Certified Information Systems Auditor*" – CISA fornecido pela ISACA.

4.2.4 Gestão da Segurança de Redes

O grupo de profissionais selecionados para a pesquisa que atua na segurança de redes é formado por especialistas com formação em ciência da

[6] ITIL - *Information Technology Infrastructure Library*

[7] COBIT - *Control Objectives for Information and Related Technology*

[8] ISACA - *Information Systems Audit and Control Association*

computação, engenharia da computação, engenharia elétrica e engenharia de redes. São responsáveis pela instalação e a atualização dos sistemas visando à manutenção da segurança das redes de computadores.

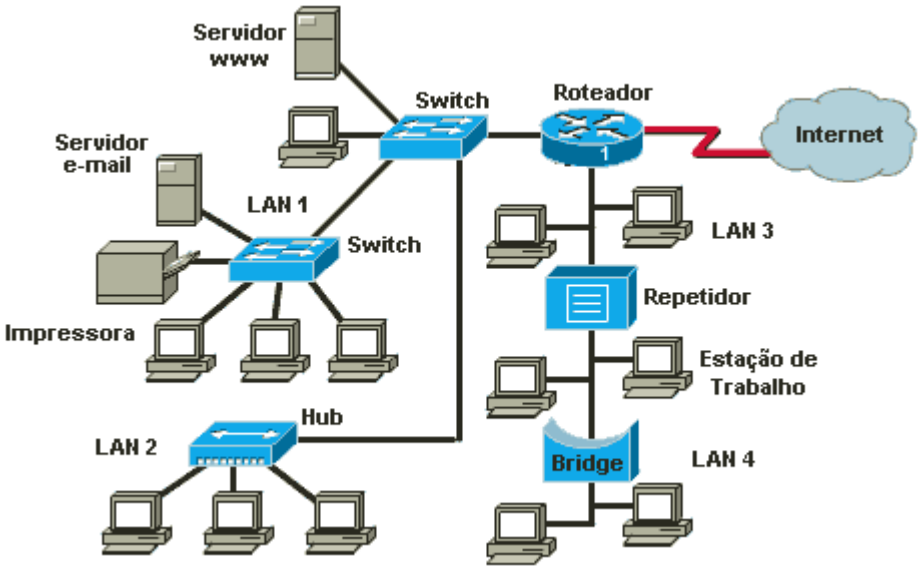

Figura 4.4 - Rede de Computadores

As redes de computadores, normalmente, envolvem o uso de servidores e computadores ligados em rede. Para operar, é necessário instalar e configurar o software de cada servidor, além de instalar e configurar o software das estações. Uma das principais tarefas do gestor é manter atualizados os programas instalados nessas máquinas. Esse trabalho é realizado por meio da instalação de versões mais novas ou por meio da aplicação de *patches*. *Patches* (em inglês, “remendo”) são programas feitos para atualizar ou corrigir os programas pré-instalados.

A instalação de um programa requer também a configuração. O processo de atualizar e corrigir falhas por meio de *patch* denomina-se gestão de atualização ou de *patches.* Em geral, os programas vêm configurados com parâmetros pré-estabelecidos pelos fabricantes. Entretanto, essas configurações nem sempre são as mais seguras. Cabe ao gestor configurá-los de forma a garantir tanto a segurança quanto o desempenho da rede. Denomina-se gestão de configuração o processo de ajustar, documentar e manter atualizada a configuração do sistema.

A operação correta dos equipamentos da rede requer o monitoramento sistemático das atividades realizadas por essas unidades. Essa operação é monitorada por meio da verificação e análise frequente dos *logs* ou registros dos sistemas. *Logs*, do inglês *log*, que significa registro, são arquivos que normalmente contêm informações sobre todas as ocorrências e eventos que afetam o funcionamento do dispositivo. Para aplicar corretamente as atualizações e correções, os gestores examinam frequentemente o conteúdo desses registros ou *logs*. Em alguns sistemas, essas informações são exibidas na tela do operador na forma de mensagens de alerta, que são exibidas no momento da ocorrência de algum evento.

A aquisição, instalação e manutenção dos equipamentos de rede dependem de uma boa especificação técnica. O profissional responsável pela escolha dos melhores equipamentos a serem adquiridos e instalados na rede, visando tanto à eficiência quanto à segurança da rede, são os especialistas em segurança de redes.

Feita a aquisição, o recebimento desse material consiste na verificação de sua conformidade e adequação, além da verificação das informações e especificações constantes nos manuais desses equipamentos. Após o recebimento, os especialistas instalam e configuram os dispositivos de rede. Em geral, uma rede é composta por são servidores, que são sistemas de computação centralizados que fornecem serviços a uma rede de computadores, ou “*storages*”, que são máquinas dedicadas exclusivamente ao armazenamento de grandes volumes de dados. A centralização dos dados nos “*storages*” também facilita o backup periódico dos dados organizacionais. Os servidores de e-mail são máquinas configuradas para armazenam e gerenciar as mensagens recebidas e enviadas pela Internet. Os *firewalls* são máquinas compostas por hardware e software específicos para a proteção das redes de computadores. Atuam como anteparos ou paredes de proteção contra invasores externos.

A administração e a manutenção dos servidores de redes envolvem a instalação e configuração desses equipamentos e a verificação periódica de seu funcionamento. Esses equipamentos estão normalmente ligados a consoles ou

monitores que exibem o estado do seu funcionamento. Por meio de softwares ou programas de computadores é possível operar e controlar as operações desses equipamentos.

A administração desses ativos envolve atividades que requerem o cadastramento e a documentação dos dispositivos ou ativos de redes. Envolve também a inspeção periódica da infraestrutura física da rede, do estado do cabeamento que interliga fisicamente as máquinas e suas respectivas conexões.

A monitoração dos ativos de rede requer a verificação do funcionamento de cada um dos elementos que compõem a rede de computadores. Os ativos de rede podem ser controlados remotamente por meio de um programa que integra o sistema de gerenciamento de redes. Normalmente, cada fabricante, tais como Cisco e HP, oferecem um conjunto de programas que são executados na estação de trabalho ou console do gestor que possui acesso remoto a todos os ativos de rede.

Cada ativo da rede deve ter seu funcionamento e desempenho monitorados. Por meio desse monitoramento, muitos problemas relacionados com atividades suspeitas são detectados. O monitoramento detecta qualquer anomalia no funcionamento do sistema, tais como o uso indevido a determinadas portas, frequência de uso de determinado recurso e tentativas sucessivas de acesso a rede mal sucedidas.

Os responsáveis pela rede de computadores, em geral, mantêm documentados os elementos que a compõem. São documentos descritivos, que incluem o diagrama da rede, dados relevantes de cada dispositivo ligado a ela, tais como o número de IP e o número de patrimônio de cada componente.

A homologação e instalação de novos recursos da rede são atividades que visam a garantir o perfeito funcionamento desses recursos. Os programas elaborados e projetados pelas áreas de desenvolvimento de sistemas são testados em ambiente controlado, especificamente configurado para testes, de forma a garantir que as configurações de segurança sejam previamente testadas. O ambiente controlado é isolado das demais redes, de forma a assegurar que durante

os testes, os equipamentos estão imunes aos ataques externos à rede. Após os testes e a homologação, os recursos são instalados no ambiente de produção.

Periodicamente, todos os eventos e ocorrências são registrados e documentados em relatórios diários não só para a manutenção dos registros e controle dos processos, como também para serem utilizados por outras equipes.

A montagem e manutenção de uma rede de computadores dependem de um bom projeto. Essa tarefa é realizada por especialistas que conhecem as demandas da organização, o funcionamento e a operação das redes. Cabe a eles especificar e selecionar os equipamentos adequados para aquisição e manutenção dessas redes.

Para manter-se atualizados, os especialistas da área de segurança de redes participam de cursos ministrados pelos fornecedores de soluções tecnológicas, tais como CISCO, DELL e HP e eventos na área de segurança da informação e cursos de especialização.

4.2.5 Principais Atividades

A Tabela 4.1 apresenta a relação das principais atividades executadas pelos especialistas e pesquisadores selecionados para a pesquisa, bem como os tipos de informação e fontes utilizados.

ATIVIDADE	TIPO DE INFORMAÇÃO	FONTES DE INFORMAÇÃO
Desenvolvimento de algoritmos e aplicativos criptográficos	Informações sobre criptografia	Livros, revistas especializadas, artigos, anais de congressos.
Desenvolvimento de hardware e firmware criptográfico.	Informações sobre circuitos, dispositivos semicondutores, compiladores.	Livros, manuais técnicos e sites especializados.
Desenvolvimento de sistemas voltados à segurança da Informação.	Informações sobre as linguagens, sistemas operacionais.	Livros, manuais técnicos e sites especializados.
Elaboração de sistemas para segurança da informação baseados em proteção de leis físicas, além de algoritmos matemáticos apoiados pela Teoria da Informação.	Informações sobre algoritmos criptográficos. Teoria da Informação.	Livros, revistas especializadas, artigos, anais de congressos.
Elaborar políticas de segurança da informação, novas estratégias de conscientização.	Informações sobre políticas, normas, leis e decretos.	Livros, normas, legislação sobre o tema.

Coordenar a resposta a incidentes, auxiliando a organização e clientes a identificar, tratar e eliminar incidentes de segurança.	Informações sobre incidentes de segurança.	Logs e sites sobre incidentes de segurança.
Instalar e configurar software, aplicar patches, gerenciar a atualização e a configuração.	Informações sobre instalação, configuração, patches disponíveis, atualizações.	Manuais de instalação, configuração, sites do fornecedor.
Monitorar operação dos sistemas de informação.	Status dos sistemas de informação.	Logs dos sistemas de informação.
Especificar software e hardware.	Informações sobre o software e sobre o hardware.	Internet, revistas especializadas.
Instalar e configurar servidores.	Informações sobre instalação e configuração.	Manuais de instalação e configuração dos servidores.
Administração, controle e manutenção monitoramento da infraestrutura de rede.	Informações sobre as atividades de cada ativo da infraestrutura de rede.	Documentação dos componentes da infraestrutura de rede, logs de redes.
Elaboração dos relatórios periódicos.	Informações para a elaboração dos relatórios.	Anotações, logs.
Planejamento, realização e execução de processos e atividades de avaliação e análise de proteção de sistemas de informação e redes computacionais.	Informações para a elaboração dos relatórios.	Documentação dos componentes da infraestrutura de rede. Documentação das instalações físicas.

Tabela 4.1 – Relação de Atividades, Tipos de Informação e Fontes.

Fonte: Dados da Pesquisa

4.2.6 Características Demográficas

Foram enviados questionários para 412 profissionais que atuam em grandes centros de pesquisas, universidades, órgãos públicos federais e estaduais da administração direta e indireta e autarquias que integram a RENASIC/COMSIC. Desse grupo de 412 profissionais integrantes da RENASIC/COMSIC, 50 responderam aos questionários. Os resultados obtidos nos questionários são apresentados a seguir:

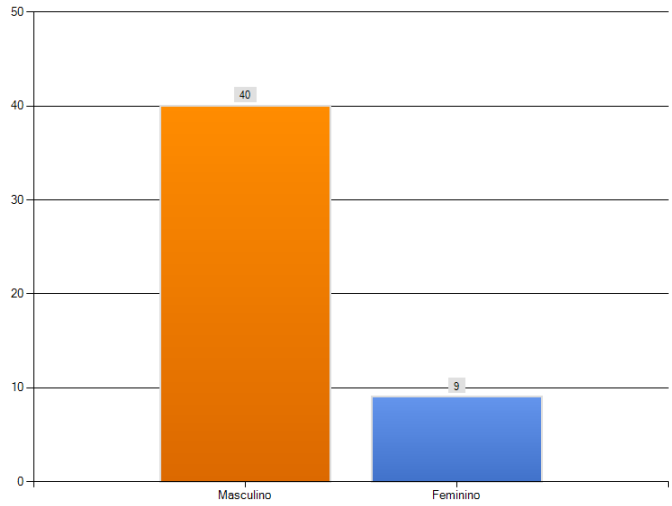

Figura 4.5 – Distribuição por Sexo

Com base na análise das respostas obtidas pode-se dizer que 82,0% (41) são do sexo masculino e 18,0% (9) são do sexo feminino.

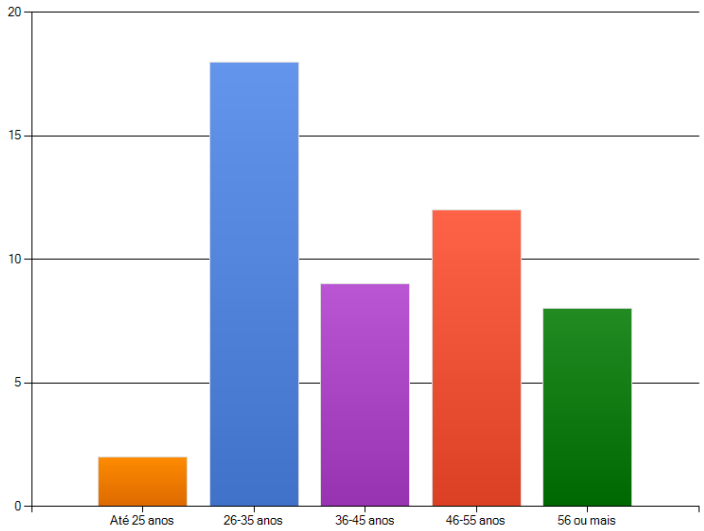

Figura 4.6 - Distribuição por Faixas Etárias

Em relação à faixa etária, apenas 4,0% (2) tem menos de 25 anos, 38,0% (19) dos pesquisados encontra-se na faixa dos 26 a 35 anos, constituindo o grupo majoritário, entre 36 e 45 anos estão apenas 18,0% (9) dos respondentes, há 24,0% (12) na faixa dos 46 a 55 e pouco menos 16,0% (8) na faixa dos 56 ou mais.

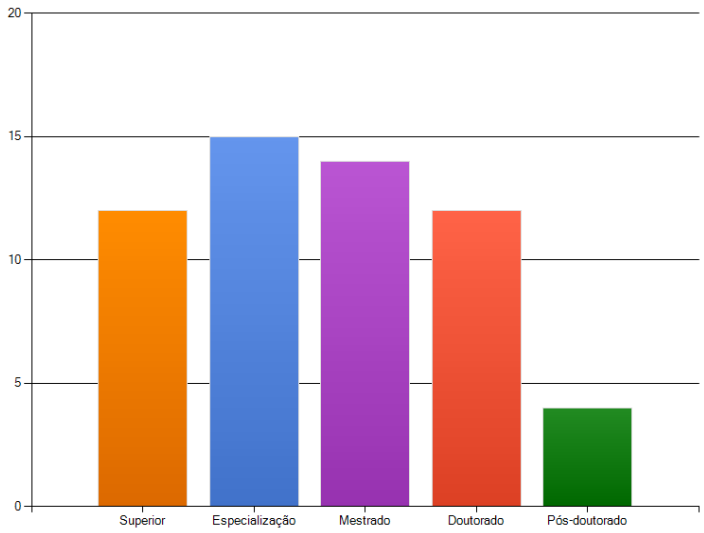

Figura 4.7 - Nível de Formação

Em relação ao nível de formação acadêmica, o grupo selecionado para a pesquisa apresenta um elevado nível de formação: 4 com pós-doutorado, 12 com doutorado, 14 com mestrado, 15 com especialização e 12 com formação superior.

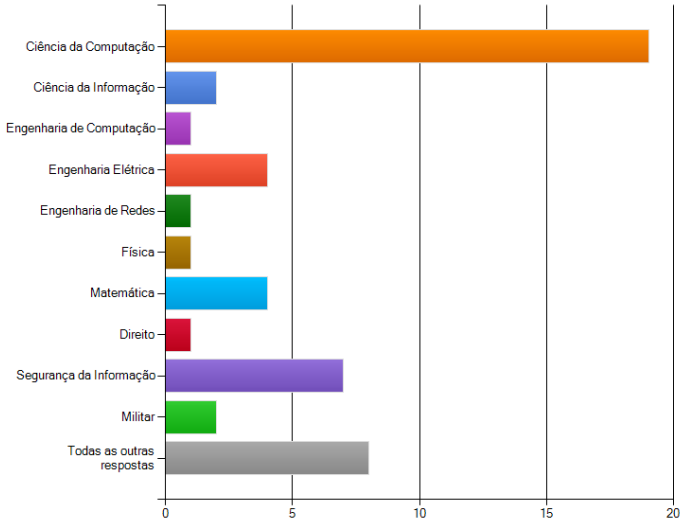

Figura 4.8 – Área de Formação

Entre os participantes da pesquisa, há profissionais renomados na área. A maior parte dos respondentes é da área da Ciência da Computação. Outras áreas de destaque são: Segurança da Informação, Engenharia Elétrica, Matemática e Estatística. Outras áreas citadas entre os respondentes são: Ótica Quântica e Criptografia Física, Estatística, Processamento de Dados, Administração de

empresas, Administração e Marketing.

Em relação à área de formação, há um predomínio de especialistas da área de ciência da computação com 38,0% (19), 16,0% (8) são profissionais de outras, 14,% (7) são especialistas em segurança da informação, 8% (4) são da área de engenharia, 8% (4) são da área de matemática, 4% (2) são militares, 4% (2) são da ciência da informação, com 2% (1) aparecem engenharia da computação, engenharia de redes, física e direito. Outras áreas citadas na pesquisa incluem: óptica quântica, criptografia física, defesa cibernética, administração, marketing, processamento de dados.

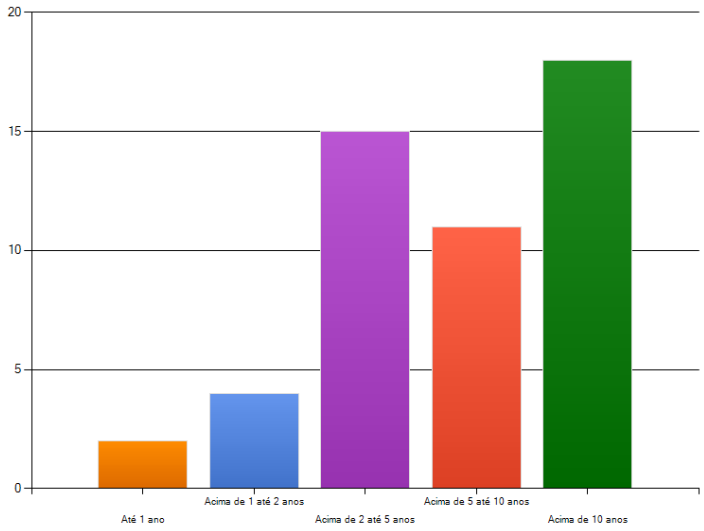

Figura 4.9 - Tempo de Experiência na Área

Em relação à experiência na área, pode-se afirmar que 8,3% trabalham na área há menos de um ano; 12,5% acima de um até dois anos; 33,5% acima de dois até cinco cincos; 16,7% cima de cinco até 10 anos e 29,2% acima de 10 anos.

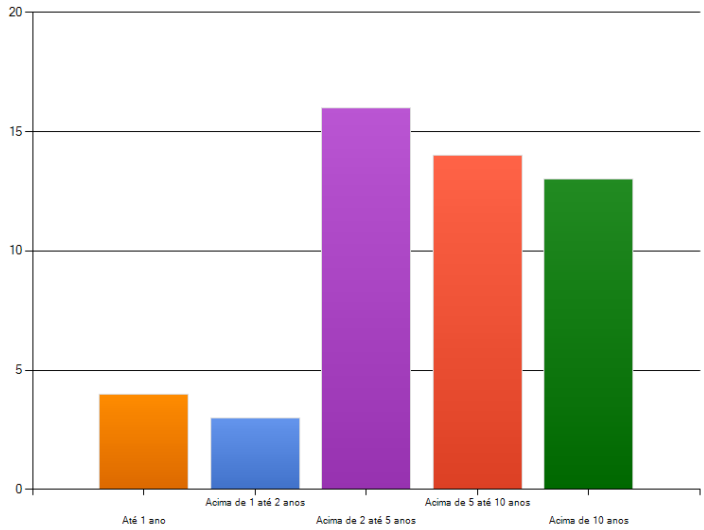

Figura 4.10 - Tempo de Experiência na Organização

O gráfico sobre o tempo de experiência na organização demonstra que 32% trabalha há menos de cinco anos na organização, 28% está na organização acima de 5 anos até 10 anos, 26% está na organização há mais de 10 anos. Esses números indicam que uma parcela significativa, isto é, 54% (27) dos respondentes, está há mais de cinco anos na mesma organização.

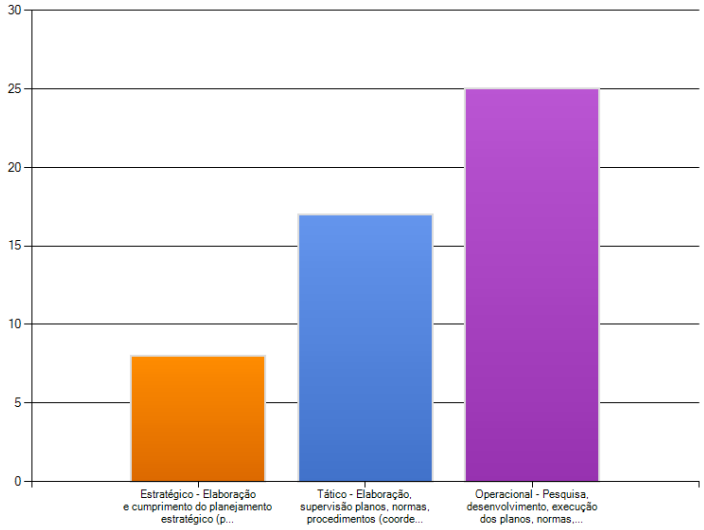

Figura 4.11 - Nível de Atuação

Foram entrevistados representantes dos três níveis organizacionais, estratégico, tático e operacional, que atuam nos setores de gestão da segurança da informação, de desenvolvimento de sistemas e projetos de segurança da informação

e algoritmos criptográficos, no setor de segurança de redes e no setor de desenvolvimento de hardware e firmware criptográficos.

Em relação ao nível de atuação, a pesquisa identificou que 16,0% (8) dos pesquisados atuam em nível estratégico ou de direção, 34,0% (17) atuam em nível tático, isto é no nível intermediário na administração e 50,0% (25) atuam em nível operacional.

4.3 As Necessidades Informacionais

No levantamento das necessidades informacionais, foram utilizados como instrumentos de coleta de dados o questionário e a entrevista semiestruturada. O objetivo foi identificar como o especialista percebe que necessita de informações. A pesquisa parte do pressuposto de que as necessidades surgem a partir das atividades realizadas por esses profissionais.

Em relação aos temas, a Tabela 4.2, sobre a frequência de busca por tema mostra que os temas mais frequentemente pesquisados pelos especialistas selecionados nesta pesquisa são a criptografia, com 32,6 % (14), em segundo lugar, a segurança das comunicações e operações, com 29,5% (13) e segurança da informação aplicada aos sistemas de informação, com 27,3 % (6). Entre os temas com menor frequência de busca estão a guerra e defesa cibernética 9,5% (4), o direito digital, com 4,9 % (2) e a perícia e a investigação de crimes cibernéticos, com 5,0% (2). Deve-se ressaltar que esses percentuais refletem as preferências de um grupo composto majoritariamente por profissionais da ciência da computação, conforme os dados mostrados pela Figura 4.5, sobre a área de formação.

Temas de interesse	Pelo menos 1 vez ao dia	Pelo menos 1 vez por semana	Pelo menos 1 vez por mês	Pelo menos 1 vez por semestre	Pelo menos 1 vez por ano	Não me interesso por esse tema
Criptografia	32,6%	18,6%	14,0%	18,6%	11,6%	4,7%
Desenvolvimento de hardware e/ou firmware criptográfico	22,0%	7,3%	7,3%	17,1%	14,6%	31,7%

Segurança das comunicações e operações (segurança de redes)	29,5%	25,0%	15,9%	20,5%	2,3%	6,8%
Análise e gestão de riscos da segurança da informação	14,0%	23,3%	25,6%	14,0%	14,0%	9,3%
Guerra e defesa cibernética	9,5%	23,8%	16,7%	16,7%	4,8%	28,6%
Perícia e investigação de crimes cibernéticos	5,0%	22,5%	12,5%	15,0%	15,0%	30,0%
Direito digital	4,9%	12,2%	12,2%	14,6%	22,0%	34,1%
Políticas, planos, normas de segurança.	16,3%	14,0%	14,0%	18,6%	20,9%	16,3%
Segurança da informação aplicada aos sistemas de informação	27,3%	27,3%	9,1%	22,7%	9,1	4,5%

Tabela 4.2– Frequência de busca por tema

4.4 O Comportamento de Busca

A pesquisa procurou identificar como esses profissionais procedem para procurar as informações necessárias para realizar seu trabalho. Na visão de Choo (2003), grupos de pessoas têm pressupostos comuns sobre a natureza de seu trabalho que influenciam o comportamento de busca de informação.

Choo (2006, p. 86) destaca que a emoção desempenha um papel fundamental durante a busca e o processamento da informação, dirigindo a atenção para informações novas, potencialmente importantes ou confirmatórias. Os estudos sobre uso da informação reconhecem que as necessidades de informação são ao mesmo tempo emocionais e cognitivas. As reações emocionais quase sempre orientam a busca de informação, canalizando a atenção, revelando dúvidas e incertezas, indicando gostos e aversões, motivando o esforço.

O método adotado para analisar o comportamento do especialista foi caracterizar as fontes de informação utilizadas, com base nos critérios de frequência, relevância e confiabilidade, conforme descritos no referencial teórico.

Essa forma de abordagem foi proposta por Auster e Choo (1994):

- Do ponto de vista da origem – Fontes internas e externas
- Do ponto de vista do relacionamento/proximidade – Fontes pessoais e impessoais

FONTES	PESSOAIS	IMPESSOAIS
EXTERNAS	Especialistas Pesquisadores Professores Funcionários de órgãos governamentais	Jornais, livros e revistas Publicações especializadas Rádio, televisão Conferências, viagens
INTERNAS	Superiores e subordinados hierárquicos Equipe de funcionários Registros pessoais	Documentação de projetos Especificações técnicas Memorandos e circulares internos Relatórios e estudos internos Biblioteca da organização Serviços de informação eletrônica

Tabela 4.3 – Fontes de Informação Organizacional

Fonte: Adaptado de AUSTER & CHOO, 1994.

Neste trabalho, foram estabelecidos como critérios os seguintes tipos de fontes:

- Fontes internas pessoais – IP
- Fontes internas impessoais – II
- Fontes externas pessoais – EP
- Fontes externas impessoais – EI

Conforme os dados da Tabela 4.4, 30,2% (13) dos respondentes consideraram o congresso Crypto 2013 extremamente relevantes e 25,6 % (11) o Eurocrypt 2013. Foram considerados relevantes, o congresso Infosec World Conference & Expo 2013, com 37,8 % (17) e o RSA Conference 2013, com 37,2% (16).

Merecem destaque nesta tabela, os eventos Gartner Security & Risk Management Summit, considerado relevante por 34,9% (15) dos especialistas, e o Public Key Cryptography 2013, por 34,1% (14).

CONGRESSO/EVENTO	Extremamente relevante	Relevante	De alguma relevância	Irrelevante	Não conheço este evento
Asiacrypt 2013	16,3% (7)	25,6% (11)	16,3% (7)	0,0% (0)	**41,9% (18)**
Crypto 2013	**30,2% (13)**	20,9% (9)	11,6% (5)	0,0% (0)	**37,2% (16)**
Cryptographic Hardware and Embedded Systems (CHES 2013)	12,2% (5)	22,0% (9)	19,5% (8)	4,9% (2)	**41,5% (17)**
Eurocrypt 2013	**25,6% (11)**	27,9% (12)	14,0% (6)	0,0% (0)	**32,6% (14)**
Gartner Security & Risk Management Summit	2,3% (1)	**34,9% (15)**	16,3% (7)	4,7% (2)	**41,9% (18)**
InfoSec World Conference & Expo 2013	6,7% (3)	**37,8% (17)**	17,8% (8)	4,4% (2)	33,3% (15)
20th International Workshop on Fast Software Encryption (FSE 2013)	9,8% (4)	26,8% (11)	17,1% (7)	0,0% (0)	**46,3% (19)**
Public Key Cryptography 2013	12,2% (5)	**34,1% (14)**	17,1% (7)	0,0% (0)	**36,6% (15)**
RSA Conference 2013	**23,3% (10)**	**37,2% (16)**	16,3% (7)	2,3% (1)	20,9% (9)

Tabela 4.4 – Congressos e Eventos

A análise por frequência é apresentada na Tabela 4.5, que mostra o percentual de frequência busca da informação, bem como a classificação do tipo de fonte, conforme o critério estabelecido por Auster e Choo (1994).

Tipos de fontes	Fonte de Informação	Diariamente	Semanalmente	Mensalmente	Semestralmente	Anualmente	Não utilizo esse tipo de fonte de informação
EI	**Sites de busca (Google, Yahoo, etc.)**	**85,3%**	8,8%	2,9%	0,0%	2,9%	0,0%
EP	**E-mail (como fonte de informação sobre segurança da informação)**	**52,9%**	23,5%	14,7%	2,9%	2,9%	2,9%
IP	**Registros ou documentos eletrônicos pessoais**	**47,1%**	14,7%	14,7%	8,8%	2,9%	11,8%
IP	**Colegas, especialistas e pesquisadores**	**44,1%**	38,2%	14,7%	0,0%	2,9%	0,0%
EI	**Sites especializados**	**41,2%**	38,2%	8,8%	8,8%	0,0%	2,9%
II	**Site corporativo interno, portal interno, wiki interna, sistema interno**	**41,2%**	11,8%	8,8%	17,6%	0,0%	20,6%
EI	**Papers**	35,3%	14,7%	26,5%	8,8%	2,9%	11,8%
EI	**Revistas e livros especializados**	32,4%	32,4%	23,5%	5,9%	2,9%	2,9%

EI	**Fóruns eletrônicos e listas de discussão**	23,5%	26,5%	17,6%	8,8%	2,9%	20,6%
EI	**Anais de congressos**	11,8%	17,6%	14,7%	26,5%	14,7%	14,7%
EI	**Congressos/workshops/cursos/eventos**	8,8%	11,8%	20,6%	26,5%	26,5%	5,9%

Tabela 4.5 - Frequência de busca por tipo de fonte de informação

A Tabela 4.6 sobre a relevância de cada tipo de fonte de informação mostra que os "colegas" são considerados a fonte mais relevante, ou extremamente relevante por 55,9% dos pesquisados. Em seguida figuram os "livros e revistas especializadas" com 50%, e pelos "artigos" e "sites especializados", com 47,1%. Como relevantes aparecem na pesquisa, "congressos, workshops e eventos", com 47,1; "sites de busca" e "fóruns e listas de discussão", com 44,1%; e "anais de congressos", com 41,2%.

Tipos de fontes (*)	Fonte de Informação	Extremamente relevante	Relevante	De alguma relevância	Irrelevante	Não utilizo esta fonte
IP	**Colegas, especialistas e pesquisadores**	**55,9%**	32,4%	11,8%	0,0%	0,0%
EI	**Revistas e livros especializados**	**50,0%**	44,1%	2,9%	0,0%	2,9%
EI	**Papers**	**47,1%**	32,4%	11,8%	0,0%	8,8%
EI	**Sites especializados**	**47,1%**	38,2%	11,8%	0,0%	2,9%
EI	**Congressos/workshops/cursos/eventos**	41,2%	**47,1%**	5,9%	0,0%	5,9%
EI	**Sites de busca (Google, Yahoo, etc.)**	38,2%	**44,1%**	14,7%	2,9%	0,0%
IP	**Registros ou documentos eletrônicos pessoais**	38,2%	29,4%	17,6%	5,9%	8,8%
EP	**E-mail (como fonte de informação sobre segurança da informação)**	35,3%	26,5%	35,3%	0,0%	2,9%
EI	**Anais de congressos**	32,4%	**41,2%**	14,7%	0,0%	11,8%
II	**Site corporativo interno, portal interno, wiki interna, sistema interno**	17,6%	23,5%	32,4%	5,9%	20,6%
EI	**Fóruns eletrônicos e listas de discussão**	14,7%	**44,1%**	20,6%	2,9%	17,6%

Tabela 4.6 - Relevância de cada tipo fonte de informação

Embora a fonte "colegas, especialistas e pesquisadores" tenha ficado em quarto lugar na tabela de frequência, ela foi considerada extremamente relevante e a mais relevante por 55,9% dos especialistas pesquisados.

A participação em “cursos e congressos” foi considerada relevante por 47,1% e os “artigos” foram considerados extremamente relevantes por 47,1 % dos respondentes.

Tipos de fontes (*)	Fonte de Informação	Extremamente confiável	Confiável	Razoavelmente confiável	Não confiável	Não utilizo esta fonte
EI	**Revistas e livros especializados**	**44,1%**	41,2%	8,8%	2,9%	2,9%
IP	**Registros ou documentos eletrônicos pessoais**	41,2%	32,4%	14,7%	2,9%	8,8%
IP	**Colegas, especialistas e pesquisadores**	32,4%	38,2%	26,5%	2,9%	0,0%
EI	**Papers**	29,4%	55,9%	8,8%	0,0%	5,9%
EI	**Congressos/workshops/cursos/eventos**	26,5%	**58,8%**	11,8%	0,0%	2,9%
EI	**Anais de congressos**	20,6%	**58,8%**	8,8%	0,0%	11,8%
EI	**Sites especializados**	11,8%	50,0%	35,3%	0,0%	2,9%
II	**Site corporativo interno, portal interno, wiki interna, sistema interno**	11,8%	41,2%	26,5%	0,0%	20,6%
IP	**E-mail (como fonte de informação sobre segurança da informação)**	11,8%	32,4%	44,1%	**8,8%**	2,9%
EI	**Fóruns eletrônicos e listas de discussão**	2,9%	26,5%	**47,1%**	**5,9%**	17,6%
EI	**Sites de busca (Google, Yahoo, etc.)**	0,0%	20,6%	**64,7%**	14,7%	0,0%

Tabela 4.7 - Confiabilidade de cada tipo fonte de informação

Em relação à confiabilidade, a pesquisa exibe os “livros e as revistas especializadas”, com um índice de 44,1%, e os “registros pessoais”, com 41,2%, como extremamente confiáveis. Os “congressos e os anais de congressos” aparecem na pesquisa como confiáveis, com 58,8%. Os “sites de busca” são considerados relativamente confiáveis por 64,7% dos respondentes. Por outro lado, o “e-mail e os fóruns” figuram entre as fontes menos confiáveis.

A pesquisa procurou identificar os sites mais relevantes para esse grupo de especialistas. O site da IACR (*International Association for Cryptologic Research*) foi considerado extremamente relevante por 20% (9) dos profissionais que responderam ao questionário e por 100% dos que atuam na área de desenvolvimento de algoritmos e protocolos criptográficos.

Figura 4.12 - Site da IACR

Fonte: IACR(2013)

Este site contém informaçõe importantes sobre criptografia, incluindo os congressos, cursos e eventos da área. O site também contém artigos e publicações importantes como o "*Journal do Cryptology*" e os anais dos eventos patrocinados pela entidade.

SITE	Extremamente relevante	Relevante	De alguma relevância	Irrelevante	Extremamente irrelevante	Não conheço este site
http://www.iacr.org - INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH	**20,0% (9)**	22,2% (10)	15,6% (7)	2,2% (1)	15,6% (7)	**24,4% (11)**
http://www.cert.org - SOFTWARE ENGINEERING INSTITUTE - CARNEGIE MELLON UNIVERSITY	17,8% (8)	**26,7% (12)**	24,4% (11)	0,0% (0)	11,1% (5)	20,0% (9)
http://www.cert.br - CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL	13,3% (6)	**37,8% (17)**	22,2% (10)	2,2% (1)	13,3% (6)	11,1% (5)
http://www.cve.mitre.org - COMMON VULNERABILITIES AND EXPOSURES - MIT	6,7% (3)	**37,8% (17)**	20,0% (9)	0,0% (0)	8,9% (4)	26,7% (12)
http://www.nic.br - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR	11,1% (5)	**33,3% (15)**	26,7% (12)	2,2% (1)	13,3% (6)	13,3% (6)
http://www.nvd.nist.gov - NATIONAL VULNERABILITY DATABASE - NIST	15,6% (7)	**40,0% (18)**	15,6% (7)	0,0% (0)	17,8% (8)	11,1% (5)

http://www.rnp.br - REDE NACIONAL DE ENSINO E PESQUISA – RNP	15,6% (7)	26,7% (12)	**33,3% (15)**	0,0% (0)	13,3% (6)	11,1% (5)
http://www.sans.org - SANS INSTITUTE - CRITICAL SECURITY CONTROLS	8,9% (4)	**28,9% (13)**	24,4% (11)	0,0% (0)	11,1% (5)	26,7% (12)
http://www.linuxsecurity.com/ - LINUX SECURITY	6,7% (3)	22,2% (10)	**24,4% (11)**	8,9% (4)	20,0% (9)	17,8% (8)
http://www.securityfocus.com - SYMANTEC CONNECT	11,1% (5)	11,1% (5)	**26,7% (12)**	4,4% (2)	24,4% (11)	22,2% (10)
http://www.exploit-db.com/ - THE EXPLOIT DATABASE	11,1% (5)	11,1% (5)	22,2% (10)	4,4% (2)	17,8% (8)	**33,3% (15)**
http://tools.cisco.com/security/center/home.x - SECURITY INTELLIGENCE OPERATIONS	2,2% (1)	15,6% (7)	24,4% (11)	2,2% (1)	24,4% (11)	**31,1% (14)**
http://packetstormsecurity.com/ - GLOBAL SECURITY RESOURCE	4,4% (2)	13,3% (6)	17,8% (8)	2,2% (1)	15,6% (7)	**46,7% (21)**

Tabela 4.8 - Sites Relevantes

Outro site considerado relevante por 40,0% dos especialistas consultados foi o NVD (*National Vulnerability Database*). O banco de dados NVD (NIST, 1999) contém dados sobre as vulnerabilidades de software, tais como a identificação CVE (MITRE, 1999), o nível de severidade e outras informações como uma descrição e as possíveis soluções para o tratamento dessa vulnerabilidade.

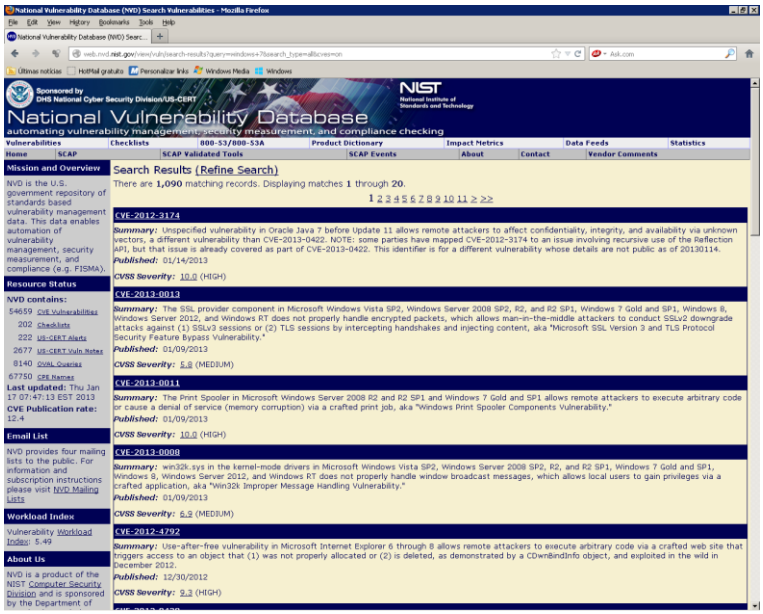

Figura 4.13 – Página do National Vulnerability Database

Fonte: National Vulnerability Database

Por meio de palavras-chave inseridas no campo de busca por palavras-chave, "*keyword search*", conforme mostra a página exibida na Figura 4.14, o usuário localiza todas as vulnerabilidades catalogadas para um determinado software. Esse banco de dados contém várias outras informações, além do

identificador, descrição e nível de severidade.Selecionando uma das vulnerabilidades encontradas, o site fornece informações mais detalhadas dessa vulnerabilidade, tais como o **vetor de acesso**, que informa se o ataque é local ou remoto; **complexidade do acesso**, que informa o nível de complexidade do ataque; **autenticação**, que informa se o sistema exige ou não a autenticação e o **tipo de impacto**, que informa quais atributos de segurança podem ser afetados e, a mais importante delas, qual a solução ou qual o controle a ser aplicado.

4.5 O Uso da Informação

Uma análise do comportamento de busca foi feita por meio de entrevistas semiestruturadas e com base nos conceitos e modelos propostos por Wilson (1999) e por Choo (2003), que utiliza o sistema de classificação de uso da informação estabelecido por Taylor (1991). A partir dos critérios de Taylor (1991), os usos da informação foram agrupados em quatro categorias principais: a) aprendizado – quando a informação foi útil para adquirir novos conhecimentos; b) resolução de problemas – quando a informação foi útil para resolver um problema específico; c) armazenamento – quando a informação foi considerada útil e foi armazenada para uso futuro e d) compartilhamento – quando a informação obtida foi compartilhada com outras pessoas, dentro e fora da organização.

A Tabela 4.9 apresenta os resultados da coleta de dados contendo os resultados sobre o uso da informação por parte dos especialistas.

Os resultados indicam que o uso mais frequente da informação é para a “solução de problemas”, com 63,6%. O uso das informações para a “solução de problemas” é também considerado extremamente relevante por 81,8% dos especialistas. O uso da informação para o “aprendizado”, ou seja, para a aquisição de novos conhecimentos que poderão ser na solução de problemas futuros, apa4rece como o segundo tipo de uso mais frequente da informação, com um índice de 59,1%. É também considerado de extremamente relevante, com 77,3 %.

A Tabela 4.10 apresenta o uso da informação classificada segundo a ordem

de maior relevância.

Uso da Informação	Diariamente	Semanalmente	Mensalmente	Semestralmente	Anualmente	Não uso as informações para esses fins
Solução de problemas	63,6%	22,7%	9,1%	0,0%	4,5%	0,0%
Aprendizado (adquirir novos conhecimentos)	59,1%	27,3%	9,1%	0,0%	4,5%	0,0%
Compartilhamento (compartilhar as informações com outros colegas e pesquisadores)	36,4%	31,8%	22,7%	4,5%	4,5%	0,0%
Armazenamento (para uso posterior e em registros pessoais)	27,3%	45,5%	18,2%	4,5%	4,5%	0,0%

Tabela 4.9 - Frequência de Uso da Informação

Os resultados demonstram que 81,8% dos pesquisados consideram o uso da informação para a “solução de problemas” extremamente relevante. Em segundo lugar figura o “aprendizado” como a forma mais relevante de uso da informação. O “armazenamento” foi considerado relevante por 50% dos pesquisados e o “compartilhamento”, por 40,9%.

Uso da Informação	Extremamente relevante	Relevante	De alguma relevância	Irrelevante	Não Uso a informação para esses fins
Solução de problemas	**81,8%**	13,6%	4,5%	0,0%	0,0%
Aprendizado (adquirir novos conhecimentos)	**77,3%**	18,2%	4,5%	0,0%	0,0%
Compartilhamento (compartilhar as informações com outros colegas e pesquisadores)	36,4%	**40,9%**	22,7%	0,0%	0,0%
Armazenamento (para uso posterior e em registros pessoais)	36,4%	**50,0%**	13,6%	0,0%	0,0%

Tabela 4.10 – Grau de Relevância

Neste capítulo foram apresentados os resultados obtidos por meio de um questionário com 21 perguntas por meio do qual foi possível identificar as necessidades, a busca e o uso da informação. A análise e a discussão, bem como os resultados obtidos por meio de entrevistas são apresentados no Capítulo 4, Análise e Discussão dos Resultados.

5 Análise e Discussão

5.1 Perfil dos Especialistas

Em relação ao perfil dos especialistas, os resultados da Tabela 4.1, que demonstra que 82,0 % dos profissionais são do sexo masculino e apenas 18,0% são do sexo feminino. Os resultados dessa tabela combinado com os resultados da Tabela 4.4, que exibe a área de ciência da computação e outras áreas das ciências exatas como as áreas dominantes entre os profissionais selecionados para a pesquisa, podem explicar o predomínio do sexo masculino nesta estatística. Esses dados contribuem para a composição do perfil do profissional, mas não há na literatura nem nas informações coletadas em campo nenhuma indicação de que essa característica influencie o comportamento de busca.

A Figura 4.3, sobre o nível de formação, exibe um número relativamente elevado de profissionais com pós-graduação. Para os profissionais selecionados para essa pesquisa, isso pode ser explicado pela necessidade de aprofundar o conhecimento teórico para atuar em determinadas áreas da segurança da informação. A área de desenvolvimento de algoritmos e protocolos criptográficos, bem como certas áreas do desenvolvimento de hardware criptográfico, tais como o de processamento de voz e de imagem exigem conhecimentos adquiridos normalmente em cursos de pós-graduação, tais como especialização, mestrado ou doutorado. Para atuar na área de gestão de segurança da informação é recomendável a capacitação desses profissionais com cursos de especialização. O nível de formação exerce influencia no tipo de informação procurada; nas fontes de informação consultadas - tais como as publicações e congressos - e no nível da informação pesquisada. Um bom exemplo da influência desse fator é a área de criptografia. Para entender certos conceitos e teorias da criptografia, tais como o emprego de curvas elípticas nos algoritmos criptográficos ou de técnicas avançadas de fatoração de números primos muito grandes, é necessário e desejável que o profissional tenha um bom conhecimento sobre álgebra e teoria dos números, em geral, adquiridos em cursos de mestrado ou doutorado, nas áreas de matemática,

estatística ou engenharia elétrica.

A Figura 4.6, sobre o tempo de experiência na organização, revela dados importantes acerca do profissional selecionado para a pesquisa. Os dados mostram que 54% dos respondentes atuam há mais de cinco anos na organização. Esse dado pode ser explicado pelo fato de a maioria dos especialistas selecionados para a pesquisa ser servidor público federal ou estadual. A estabilidade oferecida pelo serviço público faz com que esses profissionais trabalhem muito tempo na mesma organização.

O tempo de experiência na mesma organização influencia o comportamento informacional. Esse aspecto fica mais evidente nas entrevistas e na observação direta. Os profissionais com mais tempo de experiência em uma determinada organização conhecem melhor os recursos disponíveis na organização e desfrutam de maior autonomia na tomada de decisão, o que acaba influindo o comportamento de busca, exatamente por conhecerem dos recursos disponíveis, incluindo os colegas da organização, assim como pela autonomia adquirida com os anos de experiência na mesma organização.

A Figura 4.7, sobre o nível de atuação, revela que 16% atuam no nível estratégico, 34 % no nível tático e 50% no nível operacional. O nível de atuação e o papel desempenhado pelo especialista influenciam diretamente no comportamento de busca. Em geral, profissionais que atuam em cargos de direção e de gestão têm necessidades diferentes dos profissionais que atuam nos níveis operacionais. O tipo de informação de que necessitam são predominantemente de natureza administrativa que, em geral, são menos técnicas. O conhecimento técnico necessário nos casos dos profissionais que atuam no nível tático são aqueles necessários à gestão de equipes e de projetos técnicos. São responsáveis pelo planejamento e acompanhamento de projetos, pelo planejamento dos programas de formação e aperfeiçoamento técnicos de suas equipes. Também são responsáveis pela aquisição e provimento de recursos técnicos para as equipes. No caso dos profissionais que atuam no nível operacional, a natureza do trabalho realizado por esses especialistas exige um conhecimento técnico muito maior.

5.2 As necessidades Informacionais

A pesquisa analisou profissionais que atuam em três níveis organizacionais: estratégico, tático e operacional. No nível estratégico, as ações são normalmente voltadas ao planejamento estratégico da organização. As informações servem para manter o gestor em condições de tomar decisões de natureza estratégica. No nível tático, as ações estão voltadas a execução e supervisão dos planos, normas e procedimentos estabelecidos pelo nível estratégico. São também de responsabilidade do nível tático, estabelecer planos gerais de gestão da segurança da informação organizacional, incluindo a gestão de riscos, a gestão de crises e a gestão da continuidade dos negócios. No nível operacional, as situações incluem situações-problema nas quais as necessidades informacionais estão voltadas para a solução de problemas que ocorrem no dia-a-dia da organização.

Nas áreas de desenvolvimento, seja de hardware ou de criptografia, o dia-a-dia caracteriza-se pela busca de soluções que surgem em decorrência das atividades realizadas nos projetos. Há, nas fases iniciais, uma ideia geral do que se pretende atingir em termos requisitos funcionais. Nessa fase, os especialistas não sabem exatamente como resolver cada um dos problemas. Buscam informações para começar a criar um contexto, um significado e começar a compreender o problema. As necessidades, segundo a classificação de Taylor (1968), estão no nível visceral. À medida que o projeto avança, as necessidades evoluem do nível visceral para o consciente, quando já se tem consciência do que é necessário para iniciar o projeto. As primeiras buscas irão ajudar o projetista a definir melhor as funcionalidades do projeto. Chega-se ao nível formalizado, quando já se sabe exatamente como formular as questões a serem apresentadas ao sistema de informação.

Na área de segurança de redes, em geral, as necessidades já chegam formalizadas ou adaptadas. As necessidades surgem em decorrência da realização de dois tipos básicos de tarefas, embora vários outros tipos coexistam neste ambiente: aquelas decorrentes do monitoramento ou inspeção diária dos registros (*logs*) gerados pelos servidores de redes ou pela demanda gerada pelos usuários

dos sistemas. Segundo a descrição dos entrevistados, há também as demandas geradas pela necessidade de informação para a realização de tarefas de rotina como a instalação e manutenção de determinados aplicativos e sistemas operacionais.

Dependendo do tipo do problema enfrentado, o comportamento apresentado pelo especialista pode ser explicado pela metáfora da construção de sentido ("*Sense-Making*") proposto por Dervin (1983). O individuo se depara com o problema, faz uma avaliação de sua situação cognitiva e ao perceber que existe uma lacuna entre seu conhecimento atual e o conhecimento necessário para solucionar o problema, ele inicia a busca por informação para alterar seu nível de conhecimento e finalizar a tarefa. A proposta de Dervin (1983b) foi também abordada por Belkin (1980) apud Choo (2006, p.98) e denominada de "estado anômalo do conhecimento", que identifica o estado no qual o indivíduo não sabe expressar sua necessidade.

Kuhlthau apud Choo (2006, p. 99) explica esse comportamento afirmando que, devido às ambiguidades da necessidade da informação, os sentimentos de insegurança e confusão predominam nos primeiros estágios de busca. Nessas situações, o indivíduo possui uma necessidade, mas não consegue dizer, de forma precisa, o que está faltando, dificultando o uso dos sistemas de informação, que muitas vezes não estão preparados para ajudar o gestor a descrever os problemas e a identificar e caracterizar suas necessidades.

Após perceber que necessita de informação, isto é, identificada a situação do ponto de vista cognitivo de insuficiência, o indivíduo inicia a busca de informação. Para Wilson (2000), o comportamento de busca é realizado para **satisfazer uma necessidade informacional** ou **para resolver um problema específico**.

No momento em que percebe que necessita de informação, o profissional busca a informação, consulta colegas, pesquisa em sistemas de informação, procura na literatura especializada, em suma, realiza as ações que julga necessárias para encontrar as informações de que necessita.

Por fim, para concluir o ciclo proposto por Choo (2003), necessidade, busca e uso da informação, a pesquisa analisou os principais usos que o gestor faz da informação encontrada e selecionada. Na visão de Taylor (1968, 1996), há quatro elementos-chave que afetam o fluxo e o uso da informação e determinam o critério por meio do qual o valor da informação vai ser avaliado. Esses quatro elementos formam o contexto de uso da informação, a saber: grupo de pessoas, problemas típicos, ambiente de trabalho e solução de problemas.

Em relação ao uso da informação, Taylor (1996) também definiu oito classes de usos da informação: esclarecimento, compreensão do problema, instrumental, factual, confirmativa, projetiva, motivacional, pessoa ou política.

No ambiente em que os especialistas em segurança da informação selecionados para a pesquisa atuam, esses profissionais são submetidos a situações-problema. Nessas situações, as necessidades informacionais podem estar em quatro níveis, conforme a classificação proposta por Taylor: visceral, consciente, formalizado ou adaptado. Essas diferenças são fortemente influenciadas pelo tipo de tarefa executada e pelo perfil e formação do profissional.

As necessidades informacionais surgem a partir das tarefas realizadas pelos especialistas no exercício profissional e são influenciadas por diversos fatores, entre os quais o papel que ele exerce, o ambiente em que ele atua e o tipo de trabalho que ele executa.

No caso dos profissionais que atuam na segurança de redes, as necessidades informacionais estão relacionadas com a solução de problemas decorrentes das demandas geradas pelos usuários da rede, da monitoração dos ativos da rede ou de problemas que surgem a partir de atividades de rotina, tais como a instalação de programas ou de sistemas operacionais.

No caso dos profissionais que atuam em desenvolvimento de algoritmos criptográficos, as necessidades surgem, em geral, a partir da necessidade de compreender os problemas relacionados com a concepção dos projetos. Há uma concentração maior de busca de informação nas fases iniciais do projeto. Essa

demanda por informação irá declinar com o andamento do projeto. As principais fontes de informação consultadas são livros e artigos. Os congressos e seus respectivos anais são também importantes fontes de informação.

De forma análoga, os profissionais que atuam no desenvolvimento de projetos de hardware criptográfico necessitam de informações para compreender e solucionar os problemas relacionados com os projetos. As buscas por informações ocorrem com maior frequência nas fases iniciais do projeto, mas continuam durante todo o ciclo de desenvolvimento e implementação. As fontes preferenciais são os manuais técnicos obtidos por meio dos sites dos fabricantes de tecnologia. A Internet é, portanto, a fonte usada com a maior frequência. Como os projetos são feitos em equipe, há compartilhamento constante de informações com os colegas que trabalham no mesmo projeto.

Para os profissionais da gestão da segurança da informação, a necessidade e exigência de consulta a textos técnicos associados à normatização nas áreas de segurança da informação e de gestão e análise de riscos em sistemas e redes computacionais.

Conforme os dados da Tabela 4.2 sobre a frequência de busca por tema, os temas mais pesquisados são criptografia, com 32,6 %, em segundo lugar, a segurança das comunicações e operações, com 29,5% e segurança da informação aplicada aos sistemas de informação, com 27,3 %. Entre os temas com menor frequência de busca estão o direito digital, com 34,1%, a perícia e a investigação de crimes cibernéticos, com 30,0% e guerra e defesa cibernética. Esses resultados demonstram que o interesse está diretamente relacionado ao perfil, a formação e ao tipo de trabalho exercido pelo profissional. A maior parte dos respondentes é composta por profissionais da ciência da computação e atua nas áreas técnicas. Deve-se destacar o grande interesse pela criptografia não somente pelos matemáticos e estatísticos, mas também pelos demais profissionais da área.

5.3 O Comportamento de Busca

Os especialistas em segurança da informação investigados nesta pesquisa procuram informações sobre segurança da informação associadas a situações que surgem no dia-a-dia. Em todas essas situações, há um conjunto de termos, expressões ou palavras-chave relacionadas com os problemas enfrentados que podem utilizadas pelos especialistas e apresentadas aos sistemas de informação durante a busca de informação. Caso não haja uma descrição exata do problema, os termos associados poderão ser usados nas buscas iniciais. A análise das buscas iniciais e as pesquisas sucessivas permitirão o refinamento da questão a ser resolvida.

A partir análise da frequência de uso das fontes, pode-se concluir que há uma preferência pelas fontes externas e impessoais, como os “sites de busca”, seguida do uso de “e-mail”, “consulta aos registros pessoais” e a “colegas, especialistas e pesquisadores”, que são fontes internas e pessoais.

Em relação à busca de informações e às fontes de informação, os especialistas em segurança da informação citaram os próprios colegas e outros especialistas como uma das principais fontes de informação e a comunicação verbal ou escrita o meio pelo qual são obtidas as informações necessárias. Os problemas diários são encaminhados aos profissionais capacitados em solucioná-los, seja pela experiência ou por sua formação acadêmica.

Os dados da Tabela 4.6, sobre relevância das fontes de informação, indicam que “colegas, especialistas e pesquisadores” são considerados a fonte mais relevante ou extremamente relevante por 55,9% dos especialistas, embora tenha ficado em quarto lugar na Tabela 4.5, sobre frequência de uso. Isso demonstra que, embora a fonte “colegas, especialistas e pesquisadores” tenha sido considerada de extrema relevância, não é o tipo de fonte usada com a maior frequência. Os “sites de busca” como o Google, com 80%, são as fontes usadas com a maior frequência.

Esses dados corroboram com a afirmação de Choo (2003), segundo o qual os usuários obtêm informações de muitas e diferentes fontes, formais e informais.

Conforme Choo (2003), as fontes informais, inclusive colegas e contatos pessoais, são quase sempre tão importantes que as fontes formais.

Os dados da Tabela 4.6 também revelam que a “participação em cursos e congressos” foi considerada relevante por 47,1% e os “artigos” foram considerados extremamente relevantes por 47,1 % dos respondentes. Esses dados confirmam a importância que os profissionais selecionados na pesquisa, composto em sua maioria por profissionais com pós-graduação, atribuem aos congressos. Os congressos propiciam não só a busca passiva de informação, na qual o usuário atua como um receptor passivo da informação, como a busca ativa de informação, por meio do intercâmbio de informações entre os participantes do evento. As duas formas de busca de informação estão previstas no modelo de Wilson (1999), conforme mostra a Figura 2.8.

A busca de informação só ocorre nos casos em que a informação relacionada à solução do problema não é conhecida. Isso se deve, sobretudo, à falta de tempo aliada ao elevado número problemas a resolver. Se a cada problema a resolver, o especialista recorrer a fóruns e chats ocorrerá o acúmulo de tarefas. Os problemas relacionados com a segurança podem ser subdivididos em níveis de complexidade. Há os que requerem um nível de conhecimento altamente especializado e só podem ser resolvidos por um grupo restrito de especialistas, com formação superior e pós-graduação, em aqueles de menor complexidade, que requerem menor nível de especialização e formação.

Conforme a descrição do Entrevistado 4, há problemas que, independente de sua complexidade ou relevância, por ocorrerem com muita frequência, estão devidamente registrados na wiki da organização. São problemas que não exigem a busca de novas informações em fontes externas. Há problemas que devido à própria simplicidade e característica podem ser resolvidos por telefone. Outros podem ser resolvidos remotamente, por meio da rede. Há problemas que, devido à falta de informação, exigem a busca de informação em fontes externas.

Os especialistas da área de desenvolvimento de algoritmos criptográficos citaram a consulta a colegas e o compartilhamento de informações uma prática

diária e de extrema importância. Esse hábito pode ser explicado pela influência exercida pela formação acadêmica e pelas características do trabalho realizado. O trabalho executado por esses profissionais, conforme destaca o Entrevistado 6, é feito majoritariamente em equipe. São projetos de média e elevadas complexidades. Requerem um bom conhecimento de matemática e estatística. As equipes são formadas por no mínimo dois profissionais: um com pós-graduação em matemática e o outro em estatística. Dois dos três profissionais entrevistados na pesquisa possuem doutorado, o terceiro mestrado. A troca de informações faz parte do dia-a-dia das equipes de projetos.

Apesar de o colega ser a principal fonte de informação, há alguns profissionais que evitam esse tipo de consulta em determinadas situações. A razão para esse tipo de comportamento se deve ao fato de algumas pessoas não quererem demonstrar desconhecimento. Choo (2006, p.75) salienta que a escolha do canal ou fonte de informação baseia-se na comparação entre o custo do uso daquele canal e o resultado esperado daquela fonte. Para Choo, o custo é multifacetado e inclui elementos importantes como a acessibilidade física e o custo psicológico (já que pedir informação é admitir a própria ignorância, o que implica perda de prestígio ou status). O resultado é medido pela qualidade técnica ou confiabilidade da fonte.

Esse custo psicológico ou o receio da perda de prestígio dela decorrente pode constatado no depoimento de um coordenador da área de redes. Esse coordenador, Entrevistado 2, um profissional com mais de 10 anos experiência, citou um fato ocorrido com ele mesmo. Segundo seu relato, ao participar de uma reunião, um determinado tema foi tratado sem que ele tivesse conhecimento do assunto. Com receio de demonstrar desconhecimento perante os demais participantes da reunião, incluindo aqueles sob sua chefia, preferiu anotar o termo mencionado e pesquisar na Internet assim que a reunião terminasse. Esse tipo de comportamento, muito comum no dia-a-dia das organizações, acaba refletindo negativamente na produtividade interna e retardando a solução de problemas.

Em entrevista com os especialistas da área de criptografia, constatou-se que o trabalho desses profissionais é desenvolver produtos. O desenvolvimento de produtos envolve a resolução um problema matemático visando a melhoria ou o aperfeiçoamento de determinado sistema e a implementação de um determinado algoritmo. A necessidade surge quando se inicia a busca pelas melhores soluções ou pelo que existe de mais moderno em termos teóricos e pode ser usado para melhorar esse algoritmo.

Entre as principais fontes de informações consultadas, foi citado o próprio colega da mesa ao lado. Como os trabalhos são realizados em grupos, boa parte dos conceitos envolvidos em um determinado problema é discutida pelas equipes até se chegar a um consenso sobre qual a melhor solução. Outra fonte citada foram os livros. Grande parte dos livros necessários está na forma impressa e fazem parte do acervo da instituição. O entrevistado citou o caso de um livro cuja edição impressa era mais antiga, mas a informação necessária estava na versão mais recente e só havia na versão digital. A parte que interessava a eles foi então impressa antes de ser utilizada. Pode-se concluir que, entre os usuários citados na entrevista, ainda prevalece o uso de versões impressas. Perguntado se a instituição possuía o acervo necessário para as pesquisas, o Entrevistado 6 respondeu que a instituição fornecia boa parte dos livros necessários, mas que, por ser algebrista, e por lidar com Teoria dos Números, possua muitos livros sobre o tema. Como os problemas relacionados à criptografia envolvem muito conhecimento sobre Álgebra e Teoria dos Números, ele utilizava muito material de seu próprio acervo.

Quando os problemas estão relacionados com a implementação, eles recorrem aos colegas engenheiros da área de desenvolvimento de hardware e firmware criptográfico que conhecem mais sobre o assunto e conhecem uma solução mais rápida e prática para o problema.

Quando o problema se restringe a criptografia, tais como determinar: Quais critérios de segurança são necessários? Como é possível melhorar o algoritmo? Onde é possível encontrar determinado algoritmo? Nesses casos, são utilizados artigos (*papers)* e dois ou três livros. Esses artigos podem ser encontrados na

Internet. São acessados ou encontrados por meio do acesso à biblioteca da instituição ou pela biblioteca da Universidade de Brasília. O site de periódicos da Capes foi citado como fonte para a pesquisa desse material.

A consulta a artigos e periódicos vai depender da fase do projeto. Conforme relato do Entrevistado 6, a frequência de uso de determinado tipo de fonte de informação é variável e depende consideravelmente da fase em que se encontra o projeto. Essas pesquisas ocorrem com maior frequência nas fases iniciais do projeto. É na fase inicial que se concentram as pesquisas e os estudos sobre o problema. Na fase de implementação da solução, a consulta aos artigos e aos livros se reduz consideravelmente, enquanto que na fase de estudo inicial, essa consulta é diária.

O tempo dedicado aos estudos iniciais vai depender da complexidade do problema. Esse tempo pode variar de alguns dias, semanas e até alguns anos. Os projetos da área de desenvolvimento de criptografia levam em média de três meses a dois anos para serem concluídos. Há projetos que podem levar mais do que cinco anos. O tempo de desenvolvimento do projeto depende da natureza e das características desse projeto. Há projetos simples, que não requerem muita pesquisa por utilizarem informações já conhecidas. Outros, mais complexos, envolvem uma pesquisa em diversas fontes de informação. Na elaboração de um algoritmo, pode haver problemas de implementação ou de computação desconhecidos. A necessidade inicial imediata é solucionar essa questão. Os problemas vão sendo resolvidos à medida que eles surgem. O objetivo principal é o problema geral, mas para se atingir esse objetivo é necessário solucionar questões menores.

Na escolha das fontes, há critérios e análises que são feitos para se decidir por determinadas fontes. Em relação aos critérios de seleção das fontes, Choo (2006, p.100) destaca que a probabilidade de uma fonte ser selecionada depende da acessibilidade, assim como da qualidade da informação que ela vai fornecer. A acessibilidade, que implica a quantidade de esforço e tempo necessário para encontrar e usar uma fonte, é um forte indicador de que uma fonte pode ser utilizada

por muitos grupos de usuários. Em situações em que a ambiguidade é alta e a confiabilidade da informação é especialmente importante, fontes menos acessíveis e de alta confiabilidade podem ser consultadas. Durante o projeto, surge a dúvida: vale a pena seguir por este caminho? Ou seria melhor seguir por outro caminho? Às vezes é preciso experimentar determinado caminho e testar determinada solução e ver o que acontece. Muitas vezes, o caminho escolhido é mais rápido; é possível realizar com os recursos já disponíveis e ver se é possível resolver o problema. Muitas vezes, escolhe-se uma solução cujas informações não estão completamente disponíveis. Nestes casos, é mais fácil seguir um caminho a que você tenha todo o acesso do que adotar uma solução cujas informações não estão acessíveis. Às vezes uma determinada solução produz resultados excelentes, mas suas informações não estão completamente disponíveis. É melhor partir para uma solução que ofereça resultados aceitáveis, mas cujas informações estejam completamente disponíveis. O Entrevistado 6 cita um caso de uma solução de excelente qualidade, mas que dependia de uma série de informações que estavam em uma troca de e-mails entre os pesquisadores da área. Como não era possível ter acesso a esses e-mails, a solução foi abandonada e adotada outra solução, cujos resultados não eram tão eficientes, mas estavam totalmente disponíveis. Ao ser questionado sobre o que o faz desistir de uma busca, os Entrevistado 2 e 5 disseram que, em geral, quando há exigência de pagamento de custos para acesso às informações sob busca. O Entrevistado 2 acrescenta outra situação em que é obrigado a desistir da busca ou adiá-la é quando surgem problemas mais urgentes.

Na descrição de como buscava a informação, o Entrevistado 6 disse que a busca na Internet produz normalmente muitos resultados. Por exemplo, às vezes você tem um determinado problema, a busca por determinado tema produz, como resultado, um determinado artigo que passa a orientar seu trabalho. A leitura desse artigo o conduz a outros artigos por meio das referências bibliográficas. Essas referências o conduzem a outros livros e artigos. Durante a busca inicial, as fontes provavelmente vão indicar ou recomendar fontes adicionais ou referências. Seguir essas novas pistas indicadas pelas fontes iniciais é uma atividade que se chama encadear (ELLIS, 1993 apud CHOO, 2006, p.100).

O Entrevistado 7 disse que na matemática, há o site “www.ams.org/mathscinet/”. Trata-se de um site pago, de acesso restrito a assinantes, que, em geral, pode ser acessado por meio das universidades ou do portal da Capes. Neste site, é possível encontrar links para outros sites que são citados pelo site que está sendo utilizado. Algumas informações contidas nesses outros links podem se de interesse na pesquisa.

O comportamento descrito pelo Entrevistado 6 pode ser explicado pelo modelo de comportamento de busca proposto por Ellis (1989), no qual o autor classifica em oito categorias de atividades de busca informacional: iniciar; encadear; vasculhar; diferenciar; monitorar; extrair; verificar e finalizar. A categoria “iniciar” foi definida no modelo de Ellis como o conjunto de atividades que permitem uma visão geral do assunto a ser estudado, após a definição de referências que serão localizadas em primeiro lugar. Essa definição inicial pode se dar por meio de conversas com colegas, consulta à livros e publicações especializadas, catálogos on-line. Nesta pesquisa, esse padrão de comportamento foi identificado em todas as entrevistas. O início das pesquisas é caracterizado pela busca dos assuntos em bases de dados on-line disponíveis na Internet. A partir dos dados encontrados na pesquisa na Internet e das bases de on-line, os especialistas obtêm as referências iniciais de seus trabalhos. Acessam as referências e baixam os artigos que são de interesse.

Alguns entrevistados afirmaram repetir várias vezes esse comportamento inicial durante o processo de busca de informação. O comportamento do início das atividades de busca pode ser alterado pelo conhecimento prévio que o pesquisador tem do assunto a ser procurado e pela experiência no domínio das ferramentas de busca. Segundo Marchionini (1998), cada pessoa possui modelos mentais únicos, experiências e habilidades preferenciais que direcionarão a sua busca.

O conhecimento prévio e as habilidades específicas ficam claros na declaração do Entrevistado 7. Esse entrevistado afirma que quando ele não tem nenhum conhecimento prévio sobre o assunto, ele procura por palavras-chave no sistema de busca.

A confiabilidade da fonte é importante. Como a maioria dos problemas em criptografia envolvem matemática e, normalmente, os matemáticos têm por hábito provar que determinada solução é verdadeira, toda solução é previamente testada. A maioria das soluções é comprovável na prática, embora muitas vezes não seja tão simples. Há, entretanto, soluções difíceis de serem comprovadas. Nestes casos, a confiabilidade baseia-se na origem da fonte. Se ela foi publicada em um jornal de renome, se a fonte foi citada por diversos pesquisadores de renome.

Em relação ao tipo de formato ou suporte, os livros são em geral, utilizados na forma impressa, já os artigos, são obtidos tanto em revistas especializadas, quanto na Internet no formato digital. Entre as principais fontes consultadas estão o colega, a Internet, os livros e os artigos. Mesmo que a resposta não esteja na Internet, a busca vai conduzi-los a autores e a artigos. O site ou mecanismo de busca mais utilizado é o Google entre os entrevistados. Raramente se usa outro tipo de site de busca, o Entrevistado 7 afirmou que não se recordava de ter utilizado outro tipo de site de busca.

Em relação ao uso, o Entrevistado 7 disse que as informações podem ser utilizadas para solucionar problemas ou para o aprendizado de novas formas de solucionar problemas, poderão ser armazenadas para uso futuro e poderão ser compartilhadas com outros colegas. Para Marchionini (1997), a busca de informação, como aprendizagem, é um de processo cognitivo fundamental e de alto nível. A busca de informação é muitas vezes parte de aprendizagem ou de resolução de problemas. As informações obtidas durante a aprendizagem são intencionalmente armazenadas de modo que possam ser recuperadas e utilizadas em um momento posterior, no entanto, a informação adquirida como resultado da busca de informação pode ser útil para uma tarefa específica e ser descartada logo após o seu uso.

Como os trabalhos são realizados em equipe, há, na fase inicial dos estudos, intenso intercâmbio ou compartilhamento das informações entre os integrantes. Nessa fase inicial, as informações são usadas para esclarecer uma dúvida. À medida que as dúvidas vão sendo esclarecidas, obtém-se uma visão mais clara do

problema. Na fase de estudos, as busca iniciais são feitas como o intuito de aprender, para esclarecer uma dúvida. Aprende-se muito mais do que o necessário, armazena-se muita informação para ser usada no futuro, mas é necessário filtrar a informação útil e descartar uma série de informações julgadas previamente necessárias. No modelo de Ellis (1993) apud Choo (2006, p. 101), essa fase é conhecida como “diferenciação”. Nela, o indivíduo filtra e selecionada as fontes segundo a natureza e a qualidade da informação oferecida. A diferenciação geralmente depende das experiências anteriores ou iniciais com as fontes, de recomendações fornecidas por contatos pessoais e de resenhas publicadas por outras fontes.

Muitas vezes, a busca por informações ocorre pela demanda de um colega que busca uma determinada informação mais recente. Neste caso, ocorre o aprendizado especificamente para compartilhar com alguém ou esclarecer a dúvida do colega. Se o problema envolve conhecimentos de engenharia, na visão do Entrevistado 6, um engenheiro vai encontrar uma solução melhor do que um matemático, se envolve implementação, um engenheiro vai oferecer uma solução normalmente mais eficaz do que um matemático ou um estatístico. Mesmo que o engenheiro não saiba, ele busca a informação para resolver o problema demandado pelo colega da matemática. Por se tratar de uma unidade de pesquisa e reunir pessoas com diferentes formações, cabe ao matemático dar apoio aos demais integrantes nas questões que envolvem a matemática. O estatístico oferece suporte aos demais na área de estatística e, assim por diante. O setor em que atua o Entrevistado 6 é composto preponderantemente por estatísticos, seguidos pelos matemáticos, e, finalmente, por alguns engenheiros.

Para os profissionais de segurança de redes, há uma wiki interna muito eficiente na difusão da informação. O sistema é usado com muita frequência e exige uma disciplina rigorosa no cadastramento dos novos problemas e de suas respectivas soluções, sempre que novos problemas fossem identificados e suas soluções devidamente testadas.

As fontes de origem interna são as mais confiáveis do ponto de vista de sua origem. Isso ratifica os dados sobre relevância e frequência. Por serem consideradas as mais confiáveis, são as fontes utilizadas com a maior frequência e, por serem de origem interna, são normalmente bastante acessíveis. Em relação ao relacionamento e à proximidade, conforme o sistema de classificação das fontes propostas por Auster e Choo (1994) mostradas na Figura 4.3, as fontes externas e impessoais, tais como livros e revistas especializadas foram consideradas as mais confiáveis. Em relação à frequência de uso, houve um predomínio das fontes externas e impessoais, tais como os sites de busca, com 85,3 % e dos e-mails, com 52,9 %. A consulta às wikis, que guardam informações sobre procedimentos e orientações oficiais já devidamente testadas, figuram em sexto lugar, com 41,2%.

As fontes externas e impessoais foram consideradas menos confiáveis. Sendo as fontes externas e impessoais constituem a maior parte das fontes consideradas não confiáveis.

Análise	Ordem	Tipo de Fonte	Fonte de Informação	Origem Tipo	Relacionamento
Frequência	1º	EI	Sites de busca	Externa	Impessoal
	2º	EP	E-mail	Interna	Pessoal
	3º	IP	Registros ou documentos eletrônicos pessoais	Interna	Pessoal
	4º	IP	Colegas, especialistas e pesquisadores	Interna	Pessoal
	5º	II	Site corporativo interno, portal interno, wiki interna	Interna	Impessoal
Relevância	1º	IP	Colegas, especialistas e pesquisadores	Interna	Pessoal
	2º	EI	Sites especializados	Externa	Impessoal
	3º	EI	Papers	Externa	Impessoal
	4º	EI	Revistas e livros especializados	Externa	Impessoal
	5º	EI	Sites de busca	Externa	Impessoal
onfia bilida de	1º	IP	Registros ou documentos eletrônicos pessoais	Interna	Pessoal

	2º	EI	Revistas e livros especializados	Externa	Impessoal
	3º	IP	Colegas, especialistas e pesquisadores	Interna	Pessoal
	4º	EI	Papers	Externa	Impessoal
	5º	EI	Congressos/workshops/cursos/ eventos	Externa	Impessoal

Tabela 5.1- Análise da frequência, relevância e confiabilidade.

Resumidamente, há uma preferência pelas fontes externas e impessoais como os “sites de busca” e de fontes externas e pessoais como os “e-mails” A “colegas, especialistas e pesquisadores” foi considerada extremamente relevante e os “registros ou documentos eletrônicos pessoais” foram considerados os mais confiáveis.

5.4 O Uso da Informação

Os dados sobre os usos da informação mostrados pelas Tabelas 4.8 e 4.9 demonstram que nem sempre a informação considerada extremamente relevante é armazenada para uso posterior ou compartilhada com outros colegas. As informações que são armazenadas e compartilhadas com outros colegas, no caso dos especialistas em rede, conforme relato do Entrevistado 3, são aquelas relacionadas com problemas que ocorrem com muita frequência.

A segunda forma de uso mais relevante da informação foi para o “aprendizado”, demonstrando a importância e a preocupação dos especialistas pesquisados com o aprimoramento constante. O aprimoramento constante permite que os problemas sejam resolvidos com mais rapidez e facilidade, uma vez que o conhecimento de determinados assuntos evita a busca de informações. O uso para “solução de problemas” aparece na pesquisa como o tipo de uso mais frequente.

O “armazenamento para uso posterior” não aparece com muita frequência, nem foi considerado relevante e extremamente relevante pela maioria dos pesquisados. Isso se deve em parte pelo perfil dos pesquisados e do tipo de fonte utilizado. Os profissionais que utilizam preferencialmente livros e artigos, cujas

informações já estão registradas, não fazem anotações ou registros das informações buscadas.

Esse fato ficou evidente no comportamento descrito pelos especialistas da área de desenvolvimento de aplicativos e algoritmos criptográficos que, em geral, utilizam livros e artigos como principal fonte de informação. Como as informações já estão registradas em suporte permanente, o uso de recursos ou ferramentas para armazenamento e uso posterior não é uma prática de rotina, nem um procedimento sistematizado como descrito pelos profissionais da área de redes, que utilizam uma wiki para registro e compartilhamento de informações. Os especialistas no desenvolvimento de hardware e firmware, conforme o Entrevistado 9, utilizam manuais dos fornecedores disponíveis nos sites do fabricante, mas têm por hábito anotar algumas soluções em registros pessoais, tanto para consulta posterior como para a elaboração de documentação de projeto. Os especialistas em de gerenciamento de redes normalmente utilizam informações disponíveis em fóruns em listas de discussão. Nesses casos, pode ser necessário armazenar essas informações de forma segura e permanente em outro tipo de registro, seja ele pessoal ou institucional. O Entrevistado 3 disse que prefere registrar a solução a registrar apenas o endereço do site. Isso porque, segundo ele, o endereço do site pode ser alterado ou até ser removido. Mesmo no caso dos especialistas em segurança de redes, nem sempre é necessário registrar a informação antes ou depois de usar. Muitas vezes, a informação é usada e imediatamente descartada.

É importante destacar que o sistema wiki é utilizado por todos os especialistas em gestão de segurança de redes para o armazenamento e o compartilhamento das soluções encontradas. Para esses profissionais, o compartilhamento pode auxiliar na solução de diversos tipos de problemas e tornar mais ágil o trabalho da organização. O compartilhamento foi considerado relevante por 36,4 % dos participantes da pesquisa.

Na entrevista com os especialistas em segurança da informação, o uso para a solução de problemas aparece com destaque, mas ressaltam que nem sempre compartilham ou armazenam a informação para uso futuro, sobretudo, quando a

informação encontrada na busca pode ser facilmente encontrada. O Entrevistado 10 descreve o aprendizado como uma das principais formas de uso da informação. Segundo ele, os cursos e os livros são fundamentais para o exercício profissional. A atualização constante ajuda a compreender e a solucionar melhor os problemas diários. O compartilhamento ocorre com problemas considerados importantes para a maioria dos profissionais de segurança de redes. As informações sobre procedimentos relativamente complexos, ou que exigem uma série de passos, são armazenados para uso posterior sempre que se julga que se serão necessários em outras intervenções ou estão relacionados com problemas muito frequentes.

O Entrevistado 5 descreve que as informações buscadas são utilizadas para o aprendizado, com ênfase na compreensão detalhada e solução técnicas do problema existente, sempre que possível, com eventuais armazenamento e compartilhamento, dos dados e informações obtidos, com colegas de trabalho.

O uso de ferramentas para gerenciamento de documentos foi citado pelos Entrevistados 3 e 4. O armazenamento em registros pessoais demonstrou-se de uso muito frequente.

O trabalho dos profissionais de segurança da informação, conforme revelam os dados da pesquisa, caracteriza-se como uma atividade em que ocorre a criação, o uso e o compartilhamento de conhecimentos específicos para a solução de problemas. Essa é a conclusão a que se pode chegar ao examinar os índices de relevância e frequência dos itens compartilhamento, resolução de problemas e aprendizado.

Os resultados apontados pela pesquisa indicam que a maior parte dos usos que se faz da informação é para solucionar problemas. Há, entretanto, outros tipos de usos de informação que podem ser enquadrados em outras categorias propostas por Taylor (1996).

Na classificação proposta por Taylor, o uso da informação para a solução de problemas pode ser enquadrada na categoria “esclarecimento” ou “compreensão dos problemas”, já que os especialistas precisam estabelecer o contexto no qual o

problema ocorre e precisam compreender profundamente o problema a ser resolvido.

O armazenamento para uso posterior e o compartilhamento da informação podem ser enquadrados na categoria “instrumental”, uma vez que os especialistas poderão usar a informação obtida para indicar “o que fazer” e “como fazer”.

Para Gary Marchionini (1997) a busca de informação, como aprendizagem, é um de processo cognitivo fundamental e de alto nível. A busca de informação é muitas vezes parte de aprendizagem ou de resolução de problemas. As informações obtidas durante a aprendizagem é intencionalmente armazenada de modo que possa ser recuperada e utilizada em um momento posterior, no entanto, a informação adquirida como resultado da busca de informação pode ser útil para uma tarefa específica e, em seguida, descartada. As informações intermediárias ou temporariamente relevantes, muitas vezes devem ser descartadas de modo que não ocupem espaço de armazenamento ou dificultem a organização de informações armazenadas e, posteriormente, interferir com as funções de recuperação.

5.5 Aspectos Gerais do Comportamento

Choo (2003) faz algumas observações de caráter geral sobre o comportamento informacional. Para Choo, as necessidades e os usos da informação devem ser examinados dentro do contexto profissional, organizacional e social dos usuários. As necessidades de informação variam de acordo com a profissão ou grupo social do usuário, suas origens demográficas e os requisitos específicos da tarefa que ele está realizando. Esses aspectos foram detectados nesta pesquisa. Observou-se que matemáticos e estatísticos entrevistados nesta pesquisa comportam-se de forma diferente dos profissionais da engenharia e da ciência da computação.

Os matemáticos e estatísticos entrevistados, que atuam no desenvolvimento de algoritmos e protocolos criptográficos, demonstraram um interesse pela fundamentação teórica, pela demonstração, pela comprovação da teoria. Na elaboração de algoritmos e soluções que envolvem a criptografia, usam como fontes de informação, preferencialmente livros e artigos publicados em revistas especializadas. A participação de congressos nacionais e, sobretudo, internacionais, é considerada importante no processo de atualização profissional, uma vez que, nesses eventos, há um intercâmbio de conhecimento e o aprendizado de técnicas modernas.

Os engenheiros entrevistados, que atuam no desenvolvimento de hardware e firmware criptográfico, enfatizam a aplicação prática da teoria. No desenvolvimento de tecnologias para o desenvolvimento de hardware criptográfico, empregam referenciais teóricos avançados sobre tecnologias envolvendo o processamento digital de voz e imagens, reconhecimento de padrões, algoritmos implementados em hardware usando tecnologias ASIC (Applicaton Specific Integrated Circuit), CPLD (Complex Programmable Logi Device), SOC (System On Chip), tecnologias de hardware configurável tais como FPGA (Fiel Programmable Gatearry Logic) e VHDL (Hardware Description Language), cross-compilers. Buscam prioritariamente informações em sites especializados mantido pelos fabricantes e empresa de tecnologia de semicondutores. Também utilizam com menor frequência dos que os matemáticos e estatísticos os livros e os artigos (*papers*) na busca de novas tecnologias. Elaboram circuitos esquemáticos, constroem protótipos, utilizam emuladores e simuladores para testar os circuitos. Como fontes de informação sobre circuitos lógicos, utilizam manuais técnicos elaborados por fabricantes dessas tecnologias. O acesso aos sites é, em geral, gratuito, mas o acesso a determinadas informações exige o pagamento de taxas de inscrição.

Segundo Choo (2003), os usuários obtêm informações de muitas e diferentes fontes, formais e informais. As fontes informais, inclusive colegas e contatos pessoais, são quase sempre tão importantes que as fontes formais. Todos os entrevistados e praticamente todos os respondentes dos questionários relataram o uso de diversas fontes, formais e informais e destacaram a importância dos colegas

e contatos pessoais como importantes fontes de informação.

Um grande número de critérios pode influenciar a seleção e uso das fontes de informação. As pesquisas descobriram que muitos grupos de usuários preferem fontes locais e acessíveis, que não são, necessariamente, as melhores. Para esses usuários, a acessibilidade de uma fonte de informação é mais importante que sua qualidade (CHOO & AUSTER, 2003, p. 284-285, apud CHOO, 2006, p. 77). Essa preferência pelas fontes locais e acessíveis foi percebida entre os especialistas entrevistados. A consulta ao colega que trabalha na mesma seção ou na mesa ao lado são realizadas com muita frequência. A consulta aos colegas foi considerada extremamente relevante por 55,3% dos respondentes. Foi a fonte considerada a mais relevantes de todas, embora não seja a mais utilizada. O tipo de fonte utilizado com maior frequência foram os sites de busca, em particular o Google.

Segundo Kneller (1980, p.92) apud Cervo et al (20077, p.19), no processo de observação, descrição, análise, comparação e síntese das propriedades gerais e específicas dos objetos, fatos e fenômenos, a ciência encontra certas regularidades que, se uniformes, constantes e regulares, possibilitam a classificação e a generalização para objetos, fatos e fenômenos semelhantes. Alguns dos comportamentos observados na pesquisa podem ser generalizados para situações semelhantes. Um exemplo é o comportamento observado pelas equipes de projetos. Conforme os depoimentos dos entrevistados, no início do projeto as buscas de informações ocorrem com maior intensidade. Essa busca de informação que tende a declinar com o andamento do projeto. Apesar de a pesquisa ter sido feita com um grupo relativamente pequeno, tudo indica que esse comportamento pode ser generalizado outras situações semelhantes, ou seja, esse comportamento está associado ao fato de se tratar de projeto. Nos profissionais que atuam em suporte técnico de redes, essa busca de informação é mais frequente e regular ao longo do tempo.

6 Conclusão

O objetivo geral da pesquisa foi analisar o comportamento informacional dos especialistas em segurança da informação e criptografia. Para atingir esse objetivo, um grupo de profissionais membros da comunidade brasileira de segurança da informação e criptografia foi selecionado para a pesquisa. Inicialmente, identificou-se o perfil desses profissionais a partir do levantamento de alguns dados demográficos. As necessidades informacionais foram detectadas a partir das atividades realizadas no exercício de seu trabalho diário. Em seguida, avaliou-se o comportamento de busca de informação por meio da identificação das principais fontes de informação utilizadas por esse grupo de profissionais. Essas fontes foram avaliadas, segundo os critérios de frequência, relevância e confiabilidade. Para finalizar, o de uso da informação foi identificado por meio da análise do modo como os profissionais utilizam a informação selecionada.

Os dados da pesquisa demonstram que os setores em que atuam esses profissionais funcionam como unidades de informação, nas quais ocorrem a criação, o uso e o compartilhamento de informações. A pesquisa também mostra que os principais usos da informação são para a solução de problemas e para o aprendizado. O compartilhamento e o armazenamento da informação ocorrem com menor frequência, embora sejam considerados relevantes. A pesquisa também revela que os possíveis usos da informação dependem, sobretudo, do tipo e da natureza do trabalho executado.

Os diferentes modelos teóricos de comportamento informacional existentes na literatura aplicam-se ao comportamento de busca e uso de informação dos profissionais selecionados para este estudo. O modelo teórico de pesquisa proposto nesta pesquisa mostrou-se um instrumento eficaz na consecução dos objetivos da pesquisa ao auxiliar a formulação de questões que possibilitaram a identificação dos fenômenos que envolvem o comportamento informacional dos profissionais de segurança da informação.

A escolha da pesquisa mista permitiu a triangulação dos dados quantitativos obtidos por meio de questionários e da análise documental e os dados qualitativos, obtidos por meio das entrevistas. Após a coleta, análise e consolidação dos dados, foi possível concluir que os objetivos gerais e os objetivos específicos foram atingidos e que as respostas às questões da pesquisa não só foram obtidas, com também possibilitaram o surgimento de novas temáticas a serem pesquisadas em trabalhos futuros.

Os resultados da pesquisa demonstram que há um comportamento comum e diagnosticável entre os profissionais de segurança da informação. Como os profissionais que atuam na segurança da informação lidam com uma infinidade de temas, a categoria foi subdividida em subgrupos, conforme a subárea em que atuam.

O caráter multidisciplinar da segurança da informação se reflete na composição dos profissionais que atuam na área, ou seja, o grupo de especialistas selecionados para a pesquisa é composto por profissionais de diferentes áreas de formação. Essa heterogeneidade, que a princípio pareceu ser um entrave para a realização da pesquisa, demonstrou-se útil ao longo de sua realização e um fator decisivo na análise e na percepção dos diferentes comportamentos.

A partir do modelo teórico de pesquisa adotado nesse trabalho, mostrado na Figura 3.2 do Capítulo 3, foi possível diagnosticar o comportamento do grupo pesquisado e perceber que há similaridades e diferenças claras entre seus membros, devido a diversos fatores, entre os quais a natureza do trabalho realizado pelo profissional, a área de formação, o tempo de experiência, o tempo de experiência na mesma organização.

Em relação às necessidades de informação, por ser um fenômeno cognitivo não observável, ao contrário do comportamento de busca e de uso da informação, partiu-se do pressuposto de que as necessidades emergem das atividades realizadas por esses especialistas.

No caso dos profissionais que atuam na área de segurança de redes, a necessidade de informação surge a partir da demanda de um usuário da rede ou da inspeção ou da análise dos registros (*logs*) emitidos pelos dispositivos conectados à rede. Esses profissionais convivem diariamente com a solução de problemas, que tem como características básicas a instantaneidade e a urgência para serem resolvidos. As necessidades de informação surgem da necessidade de encontrar informações que auxiliem a solução desses problemas. Para resolvê-los esses profissionais compartilham e registram as soluções encontradas. As informações envolvem procedimentos e soluções encontrados em fóruns, listas de discussão ou sites especializados.

No caso dos profissionais que trabalham com desenvolvimento de projetos de médio e longo prazo, as buscam ocorrem com maior intensidade nas fases iniciais do projeto. É também nessa fase que ocorrem o compartilhamento e a disseminação das informações com os demais membros da equipe. Em geral, essas informações já estão registradas em livros, artigos e manuais, não havendo a necessidade do armazenamento para uso posterior. A necessidade de registro é necessária somente para a elaboração da documentação de projetos. Em síntese, pode-se dizer que o comportamento de busca e uso da informação está diretamente ligado às fases do projeto e está diretamente associada à natureza do trabalho.

Os profissionais de gestão da segurança da informação entrevistados na pesquisa são responsáveis por todas as tarefas relacionadas com a manutenção da segurança da informação. A característica principal dos profissionais selecionados na pesquisa é lidar com vários tipos de problemas. Eles são responsáveis pela elaboração de políticas que, à semelhança daqueles que atuam em desenvolvimento de projetos, concentram suas buscas no início da elaboração da política e seguem os padrões de comportamento de busca proposto por Ellis (1989). Esses especialistas são também demandados quando ocorre um incidente de segurança. Sempre que ocorrem falhas na segurança, esses profissionais são notificados. Cabe a eles buscar informações para solucionar os problemas ou, em determinados casos, encaminhar os problemas aos setores que tenham condições técnicas de atender àquela demanda.

A busca de informação utiliza fontes internas e externas, pessoais e impessoais. A pesquisa apontou como frequente o uso de sites de busca na Internet, embora a consulta a colegas tenha se caracterizado entre as mais fontes mais relevantes. Mais uma vez, a consulta a colegas só não foi considerada a mais frequente devido à influência da natureza do trabalho. Tanto os especialistas em redes quanto os especialistas que atuam na área de desenvolvimento descrevem a consulta a colegas e o compartilhamento de informações como relevantes. A frequência, entretanto, dependerá, no caso do desenvolvimento, da fase em que se encontra o projeto.

Em relação ao comportamento de uso da informação, a pesquisa revelou que o uso mais frequente da informação é para a “solução de problemas” e para o “aprendizado”. O “compartilhamento” e o “armazenamento” da informação ocorrem com muita frequência entre os especialistas que atuam na área de redes. Esse compartilhamento e armazenamento são feitos por meio de bancos de dados internos da organização, nos quais são registrados os problemas e as respectivas soluções. A pesquisa também revelou que muitos profissionais da área de matemática e estatística, que desenvolvem algoritmos criptográficos, fazem uso intensivo de livros e artigos e preferem o material impresso ao material no formato digital.

Algumas observações de caráter geral sobre o comportamento informacional devem ser destacadas. As necessidades e os usos da informação devem ser examinados dentro do contexto profissional, organizacional e social dos usuários. As necessidades de informação variam de acordo com a profissão ou grupo social do usuário, suas origens demográficas e os requisitos específicos da tarefa que ele realiza.

A pesquisa também permitiu observar que matemáticos e estatísticos avaliados neste trabalho comportam-se de forma diferente dos profissionais da engenharia e da ciência da computação.

Os matemáticos e estatísticos demonstraram um interesse pela fundamentação teórica, pela demonstração, pela comprovação da teoria. Na

elaboração de algoritmos e soluções que envolvem a criptografia, usam como fontes de informação, preferencialmente, livros e artigos publicados em revistas especializadas. A participação de congressos nacionais e, sobretudo, internacionais, é considerada importante no processo de atualização profissional, uma vez que, nesses eventos, há intercâmbio de conhecimento e aprendizado de técnicas modernas.

Os engenheiros consultados nesta pesquisa, que atuam no desenvolvimento de hardware e firmware criptográfico, enfatizam a aplicação prática da teoria. No desenvolvimento de tecnologias para o desenvolvimento de hardware criptográfico, empregam referenciais teóricos sobre diversos tipos de tecnologias tais como o processamento digital de voz e imagens, reconhecimento de padrões, algoritmos implementados em firmware ou em hardware usando tecnologias de circuitos integrados com lógica programável tais como o FPGA. Buscam prioritariamente informações em sites especializados mantido pelos fabricantes e empresa de tecnologia de semicondutores. Também utilizam com menor frequência dos que os matemáticos e estatísticos os livros e os artigos na busca de novas tecnologias. Utilizam prioritariamente manuais técnicos elaborados por fabricantes dessas tecnologias. O acesso aos sites é, em geral, gratuito, mas algumas publicações são vendidas pelos fabricantes.

Os usuários obtêm informações de muitas e diferentes fontes, formais e informais. As fontes informais, inclusive colegas e contatos pessoais, são quase sempre tão importantes quanto as fontes formais. A escolha das fontes é influenciada por uma série de critérios, entre os quais se destaca a acessibilidade das fontes. A rapidez e o acesso fácil justificam essa preferência pelas fontes locais e acessíveis.

No processo de observação do comportamento informacional, é possível encontrar certas regularidades que, por serem bastante uniformes, possibilitam a generalização. Alguns dos comportamentos observados nos profissionais selecionados na pesquisa podem ser generalizados. Um exemplo é o comportamento observado naqueles que atuam em projetos. Segundo os

entrevistados, as buscas intensificam-se no início do projeto e tendem a declinar no seu decorrer. No caso dos profissionais que atuam em suporte técnico de redes, essa busca de informação é constante e regular ao longo do tempo.

A partir da identificação desse comportamento, de como surgem as necessidades informacionais, de como buscam a informação, quais são as fontes de informação utilizadas, quais os critérios utilizados para selecionar essas fontes e quais os possíveis usos da informação, foi possível verificar que esse comportamento não só é diagnosticável, como também pode melhorado.

Os resultados permitem concluir que é possível melhorar o acesso desses profissionais à informação de que necessitam, disponibilizando os recursos e as fontes mais relevantes e confiáveis, bem como criando portais que reúnam todas as informações, referenciais bibliográficos e links que permitam encontrar essas informações.

Conhecer as necessidades informacionais possibilita a adequação dos acervos informacionais das bibliotecas organizacionais de forma a atender não só às necessidades gerais desses profissionais, como também à demanda por informações específicas.

Já o planejamento permite que os investimentos sejam feitos de forma racional, priorizando a aquisição das publicações de uso mais frequente, a assinatura das publicações e dos sites mais importantes. A partir dos dados coletados na pesquisa também é possível criar planos e programa de treinamento visando atender às necessidades de informação desses usuários.

Os resultados da pesquisa também podem subsidiar a elaboração e planos e políticas públicas para o setor de segurança da informação e a realização de trabalhos futuros.

Entre as possíveis pesquisas a serem realizadas em trabalhos futuros incluem-se os estudos aprofundados sobre as fontes de informação utilizadas por profissionais da segurança da informação.

Os resultados obtidos, sobretudo nas entrevistas, demonstram que existe uma infinidade de fontes consultadas por esses profissionais, mas não existe uma uniformidade nem uma unanimidade sobre que fonte é a mais importante.

Outra pesquisa de interesse desses profissionais seria um estudo que possibilitasse identificar e classificar as principais fontes de informação, segundo a frequência de acesso. Esse levantamento permitiria o desenvolvimento de um sistema de informação baseado em conceitos usados em sistemas adaptativos. Esses sistemas se reconfigurariam automaticamente e se adaptariam ao perfil do usuário. À medida que o usuário realizasse as buscas, o sistema recolheria as informações de frequência ou as preferências dos usuários e se reconfiguraria de forma a adaptar-se aos hábitos desse usuário. Dessa forma, o sistema poderia classificar as fontes e os temas segundo alguns critérios, tais como a frequência de uso e o tempo de permanência naquela determinada fonte, que poderiam ser usados como indicadores de sua relevância ou qualidade. Em suma, desenvolver sistemas de informação mais bem adaptados às necessidades, ao comportamento de busca e de uso da informação desses profissionais.

Outra sugestão de pesquisa futura seria a criação ou a unificação dos modelos teóricos de comportamento informacional e das métricas ou indicadores de avaliação da qualidade das fontes, de forma a permitir que os resultados alcançados nas pesquisas possam ser comparados entre si ou usados como parâmetros de referência ou como indicadores de adequação dos serviços de informação.

Para finalizar, acredita-se que os dados e as sugestões apresentados nesta pesquisa podem representar uma importante contribuição para a ciência da informação, de forma geral e, em particular, para os estudos sobre comportamento informacional dos profissionais que atuam em segurança da informação.

7 Referências Bibliográficas

AUSTER, E.; CHOO, C. W. CEOs, **Information, and Decision-making: Scanning the Environment for Strategic Advantage**, Library Trends, v.43, n.2, p.206-225, Fall 1994.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2008.

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, p168-184, maio/ago. 2007.

BELKIN, Nicholas J. **Anomalous States of Knowledge as a Basis for Information Retrieval.** Canadian Journal of Information Science, v.5, p. 133-143, 1980.

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

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

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

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: < http://www.cert.br/stats/incidentes/ >. Acesso em: 26 jun. 2013

CERVO, A. L. et al **Metodologia Científica**. 6ª ed. São Paulo: Pearson Prentice

Hall, 2007.

CHOO, C.W. **A Organização do Conhecimento: Como as Organizações Usam a Informação para Criar Significado, Construir Conhecimento e Tomar Decisões**. São Paulo: Editora Senac São Paulo, 2003.

_____(1999). **Closing the Cognitive Gaps: How People Process Information**. Disponível em: <http://choo.ischool.utoronto.ca/FIS/respub/FThis/default.html>. Acesso em: 05 dez 2012.

_____(2000). **Information Seeking and Knowledge Work on the Wolrd Wide Web**: Kluwer Academic Press, 2000, p.8

CHOO, C.W. DETLOR, B.; TURNBULL, D. **A Behavioral Model of Information Seeking on the Web**. 1998. 1998 ASIS Annual Meeting Contributed Paper. Disponível em: <http://www.ischool.utexas.edu/~donturn/papers/asis98/asis98.html>. Acesso em: 29 set. 2012.

CRESWELL, J.W.; CLARK, V.L. **Designing and Conducting Mixed Method Research**. USA: SAGE, 2007. 275p.

CRUZ, F.W. **Um Modelo para Mapeamento de Necessidades e Usos de Informação Musical.** Revista Ciência da Informação, v.16, n.2 Belo Horizonte abr./jun. 2011.

DEMO, P. **Pesquisa e Construção de Conhecimento**. Rio de Janeiro: Tempo Brasileiro, 1996.

DERVIN, Brenda. **An Overview of Sense-Making Research: Concepts, Methods and Results to Date**. In: INTERNATIONAL COMMUNICATIONS ASSOCIATION

ANNUAL MEETING. Dallas, may, 1983.

DERVIN, Brenda; NILAN, M. **Information Needs and Uses**. In: WILLIAMS, M. (Ed.). In: Annual Review of information Science and Technology. v. 21. p. 3-33. 1986.

DERVIN, Brenda. **User as Research Inventions: How Research Categories Perpetuate Inequality**. Journal of Communications. v.39, n.3, p.216-232, 1989.

DERR, R. L. **A Conceptual Analysis of Information Need. Information Processing and Management**, v. 19, n. 5, p. 273-278, 1983.

DIAS, Maria Matilde; PIRES, Daniela. **Usos e Usuários da Informação**. São Carlos: Edufscar, 2006.

ELLIS, D. (1992): **Paradigms and proto-paradigms in information retrieval research**. En: Pertti, Vakkari, Blaise Cronin (Eds.): Conceptions of Library and Information Science. Historical, empirical and theoretical perspectives. London, 165-186.

ELLIS, David. **A Behavioral Approach to Information Retrieval System design**. Journal of Documentation. London. v.45, n.3, p.171212, Sep.1989.

FERREIRA, Sueli Mara Soares Pinto. **Novos Paradigmas e Novos Usuários de Informação.** Ciência da Informação, Brasília, v.25, n.2, p.1-10, 1995. <http://bogliolo.eci.ufmg.br/downloads/TGI004%20Sueli%20Ferreira.pdf>

FERREIRA, Sueli Mara Soares Pinto. **Estudos de Necessidades de Informação: dos Paradigmas Tradicionais à Abordagem Sense-Making.** Porto Alegre: ABEBD, 1997. 29 p.

FERREIRA, Sueli Mara S. P. **Estudos de Necessidades de Informação: dos**

Paradigmas Tradicionais à Abordagem Sense-Making (2002). Disponível em: <www.eca.usp.br/nucleos/sense/index.htm>. Acesso em: 14 jan. 2012.

_____. **Novos paradigmas de informação e novas percepções de usuários**. Ciência da Informação, Brasília, DF, v. 25, n.2, p. 217-223, maio/ago. 1996. [Links]

FERREIRA, S. M. P.; PITHAN, D. N. **Estudos de Usuários e de Usabilidade na Biblioteca INFOHAB: Relato de uma Experiência**. Disponível em: <http://eprints.org.archive/00011621/01Microsoft_Word_-_SIDI.2005_FerreiraPithan_15.outubro.pdf >. Acesso em: 20. jan. 2008. [Links]

FIGUEIREDO, Nice Menezes de. **Estudos de Uso e Usuários da Informação**. Brasília: IBICT, 1994. 154 p.

FIGUEIREDO, Nice Menezes de. **Estudos de Uso e Usuários da Informação**. Brasília: IBICT, 1994. 154 p.

FIGUEIREDO, N. M. **Serviços de Referência & Informação**. São Paulo: Polis, 1992. 167 p.

_____ Usuários. In: _____ **Paradigmas Modernos da Ciência da Informação**. São Paulo: Polis/APB, 1999. p. 11-33.

FIGUEIREDO, R. C. **Estudo Comparativo de Julgamentos de Relevância do Usuário e Não-Usuário de Serviços de Disseminação Seletiva da Informação**. Ciência da Informação; v. 7, n. 2, p. 69-78, 1978.

FIGUEIREDO, N. M. de. Usuários. In: _____. **Paradigmas modernos da Ciência da Informação em usuários/coleções/referência & informação.** São Paulo: Polis : APB, 1999.p. 11-54.

FONTES, E. **Segurança da Informação: O Usuário Faz a Diferença**. São Paulo: Saraiva, 2006.

GASQUE, Kelley Cristine Gonçalves Dias. **Comportamento dos Professores da Educação Básica na Busca da informação para Formação Continuada**. 2003. Dissertação (Mestrado em Ciência da Informação) - Departamento de Ciência da Informação, Faculdade de Estudos Sociais Aplicados, Universidade de Brasília, Brasília, 2003.

GASQUE, K. C. G. D.; COSTA, S. M. S. C. **Comportamento dos Professores da Educação Básica na Busca da Informação para Formação Continuada**. Revista Ciência da Informação, v.32, n.3 Brasília set./dez. 2003.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 1999.

IACR (2013). **International Association for Cryptologic Research**. Disponível em: <>. Acesso em: 05 mai. 2013.

JOHNSON, R. B; ONWUEGBUZIE, A. J.; TURNER, L. A. **Toward a Definition of Mixed Methods Research**. Journal of Mixed Methods Research, v.1, p.112–133, 2007.

KUHLTHAU, C. **A Principle of Uncertainty for Information Seeking**. Journal of Documentation, v. 49, n.4, p.339-355, 1993.

KUHLTHAU, Carol. **The role of experience in the information search process of an early career information worker: perceptions of uncertainty, complexity, construction and sources**. Journal of the American Society of Information Science. v. 50, n. 5, p.399-412, 1999.

KVALE, S. Interviews: **An Introduction to Qualitative Research Interviewing**.

Thousand Oaks. SAGE. 1996. 344 p.

LE COADIC, Y. **A Ciência da Informação**. Brasília: Briquet de Lemos, 2004.

MARCHIONINI, G. **Information Seeking in Electronic Environments**. Cambridge: Cambridge University Press, 1997. Cap. 1. Disponível em: http://www.ils.unc.edu/~march/isee_book/Chapter_1.pdf>. Acesso em: 2 out. 2012.

MARTINEZ-SILVEIRA, Martha, ODDONE, Nancy. **Necessidade e Comportamento Informacional: Conceituação e Modelos**. Revista Ciência da Informação, vol. 36, n.2, Brasília, maio/agosto, 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.

_____. **Identificação de necessidades de informação e sua relação com as competências informacionais: o caso da supervisão indireta de instituições financeiras no Brasil**, 2007. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2007.

MITRE Corporation. **CVE - Common Vulnerabilities and Exposures.** (1999). Disponível em:< http://cve.mitre.org/>. Acesso em: 16 jun. 2010.

MITRE Corporation.2007. **Terminology**. Disponível em: <http://www.cve.mitre.org/about/terminology.html>. Acesso em: 07 abr. 2011

MORSE, J. **Principles of Mixed Methods and Multimethod Research Design**, In: Tashakkori, Abbas, Teddlie, Charles Editor. Handbook of Mixed Methods in Social & Behavioral Research. Thousands Oaks: Sage Publications, p.189-208, 2003.

NADAES, Adriana Duarte, ANDRADE, Afonso Victor. **Necessidade, Busca e Uso da Informação: Um Olhar Voltado para a Monitoração Ambiental**. Revista de Ciências Gerais, Vol. 4 nº 19, Ano 2010.

NEHMY, R. M. Q., PAIM, I. **A Desconstrução do Conceito de "Qualidade da Informação".** Ciência da Informação, v.27, n.1, p. 36-45, 1998.

NIST. **NIST SP 800-30 Risk Management Guide for Information Technology Systems**. Disponível em: < http://csrc.nist.gov/publications/ nistpubs/800-30/sp800-30.pdf>. Acesso em: 5 ago. 2010.

NIST. **National Vulneralibility Database**.(1999). Disponível em: <http://nvd.nist.gov/>. Acesso em: 10 jun. 2010

NIST. **NIST SP 800-30 Risk Management Guide for Information Technology Systems**. Disponível em: < http://csrc.nist.gov/publications/ nistpubs/800-30/sp800-30.pdf>. Acesso em: 5 ago. 2010.

OLIVEIRA Jr., C. D.; MOREIRA, L. N.; SANTOS, T. F., NASCIMENTO, G. F. **O Conceito de Relevância e o Feedback do Usuário Final do Repositório Institucional da Universidade de Brasília (2011)**. Disponível em: <http://seer.bce.unb.br/index.php/RICI/article/view/6213>. Acesso em: 17 jan. 2013.

PEREIRA, F. C. M. **Comportamento Informacional na Tomada de Decisão: Proposta de Modelo Integrativo**. Tese apresentada ao programa de pós-graduação em Ciência da Informação da Universidade Federal de Minas Gerais, Belo Horizonte, 2011.

PEREIRA, J. C. L. **Necessidade, Busca e Uso da Informação: Estudo de caso em um Setor de Help Desk de Indústria Cimenteira Multinaciona**l. Dissertação de mestrado apresentada ao programa de pós-graduação em Ciência da Informação

da Universidade Federal de Minas Gerais, Belo Horizonte, 2008

PINHEIRO, L. V. R **Informação: esse Obscuro Objeto da Ciência da Informação**. Morpheus, Rio de Janeiro, Ano 2, nº 4, 2004. Disponível em: < http://www.unirio.br/morpheusonline/Numero04-2004/lpinheiro.htm>. Acesso em: 16 mai. 2013.

QUIVY, R.; CAMPENHOUDT, L. V. **Manual de Investigação em Ciências Sociais**. Lisboa: Gradiva, 1992.

RENASIC (2008). **Rede Nacional de Segurança da Informação e Criptografia**. Disponível em: < www.renasic.org.br/ >. Acesso em: 5 de maio de 2013.

RICHARDSON, R. J. et al. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 1999.

SARACEVIC, Tefko. **Ciência da Informação: Origem, Evolução e Relações**. Perspectivas em Ciência da Informação, Belo Horizonte, v.1, n.1, p41-62, jan/jun.1996.

SARACEVIC, Tefko. **Relevance Reconsidered. In: Information science: Integration in Perspectives**. Proceedings of The Second Conference on Conceptions of Library and Information Science (COLIS 2), p. 201-208, October, 1996.

SCHAMBER, L.; EISENBERG,M.; NILAN, M. **A Re-examination of Relevance: Toward a Dynamic, Situational Definition**. Information Processing and Management, v. 26, n. 6, p.755-776, 1990.

SÊMOLA, M. **Gestão da Segurança da Informação: Visão Executiva da Segurança da Informação**. Rio de Janeiro: Elsevier, 2003.

SILVA, T. E.; TOMAEL, M. I. Gestão da Informação nas Organizações. Revista Informação & Informação, n. 12. Londrina: Universidade Estadual de Londrina, 2007.

SOUTO, L. F. **Informação Seletiva, Mediação e Tecnologia: A Evolução dos Sistemas de Informação Seletiva de Informações**. Rio de Janeiro: Interciência, 2010.

STAREC, C.; GOMES, E.; BEZERRA, J. (org.). **Gestão Estratégica da Informação e Inteligência Competitiva**. São Paulo: Saraiva, 2006.

TAYLOR, R. S. **Question Negotiating and Information Seeking in Libraries**. College & Research Libraries, v.28, p.178-194, 1968.

_____. **Information Use Environments**. In: AUSTER, E., CHOO, C. W. (Eds.) Managing Information for the Competitive Edge. New York: Neal-Schuman, p. 93-135, 1996

TERUEL, A. G. **Los Estudios de Necesidades y Usos de la Información:** Fundamentos e Perspectivas Actuales. Gijón: Ediciones Trea, 2005. 181 p.

TRINTA, F. A., MACEDO, R. C. **Um Estudo sobre Criptografia e Assinatura Digital**. Disponível em : < http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm >. Acesso em: 28 mai. 2013.

VIEIRA, T. M. **O Direito à Privacidade na Sociedade da Informação: Efetividade Desse Direito Fundamental Diante dos Avanços da Tecnologia da Informação**. Porto Alegre: Sergio Antônio Fabris Ed., 2007.

VALENTIM, M. (org.). **Gestão, Mediação e Uso da Informação**. São Paulo: Cultura Acadêmica, 2010.

WILSON, T. D. **Models in Information Behavior Research**. Journal of Documentation, v. 55, n. 3, June 1999, p. 249-270.

WILSON-DAVIS, K. **The Center for Research on Users Studies: Aims and Functions**. Aslib Proceedings, v. 29, n. 2, p. 67-76, 1977.

WILSON, T. D., WALSH, C. (1996). **Information Behavior: An Inter-Disciplinary Perspective**. Disponível em: <http://informationr.net/tdw/publ/infbehav/index.html>. Acesso em: 05 Dec 2012.

WILSON, T. D. **On User Studies and Information Needs**. Journal of Documentation, v. 31, n. 1, p. 3-15, 1981.

WHITMAN, M.E., MATTFORD, H.J. **Principles of Information Security**. 4th Edition.

Anexo A – Questionário

Universidade de Brasília

COMPORTAMENTO INFORMACIONAL DE ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA

PARTE 1 - PERFIL DO ESPECIALISTA

Identificação.

Nome _____

E-mail _____

Telefone _____

Nome da instituição (em que trabalha).

_____

Sexo.

☐ **Masculino** ☐ **Feminino**

Idade.

☐ **Até 25 anos**
☐ **26 – 35 anos**
☐ **36 – 45 anos**
☐ **46 – 55 anos**
☐ **Acima de 56 anos**

Nível de formação.

☐ **Superior**
☐ **Especialização**
☐ **Mestrado**
☐ **Doutorado**
☐ **Pós-doutorado**

Área de formação.

- ☐ **Ciência da Computação**
- ☐ **Ciência da Informação**
- ☐ **Engenharia da Computação**
- ☐ **Engenharia Elétrica**
- ☐ **Engenharia de Redes**
- ☐ **Outra área**

  Especifique: _____
- ☐ **Física**
- ☐ **Matemática**
- ☐ **Direito**
- ☐ **Segurança da informação**
- ☐ **Militar**

Há quanto tempo trabalha com SEGURANÇA DA INFORMAÇÃO ou CRIPTOGRAFIA?

- ☐ **Até 1 ano**
- ☐ **Acima de 1 até 2 anos**
- ☐ **Acima de 2 até 5 anos**
- ☐ **Acima de 5 até 10 anos**
- ☐ **Acima de 10 anos**

Há quanto tempo trabalha nesta organização?

- ☐ **Até 1 ano**
- ☐ **Acima de 1 até 2 anos**
- ☐ **Acima de 2 até 5 anos**
- ☐ **Acima de 5 até 10 anos**
- ☐ **Acima de 10 anos**

Nível de atuação.

- ☐ **Estratégico**
- ☐ **Tático**
- ☐ **Operacional**

PARTE 2 – NECESSIDADE DE INFORMAÇÃO DO ESPECIALISTA

Cite um ou mais temas de maior interesse (área de concentração de seu trabalho).

	Pelo menos 1 vez por dia	Pelo menos 1 vez por semana	Pelo menos 1 vez por mês	Pelo menos 1 vez por semestre	Pelo menos 1 vez por ano	Não me interesso por esse tema
Criptografia	☐	☐	☐	☐	☐	☐
Desenvolvimento de hardware e software criptográfico	☐	☐	☐	☐	☐	☐
Segurança das comunicações e operações	☐	☐	☐	☐	☐	☐
Análise e gestão de riscos da segurança da informação	☐	☐	☐	☐	☐	☐
Defesa cibernética	☐	☐	☐	☐	☐	☐
Investigação de crimes cibernéticos	☐	☐	☐	☐	☐	☐
Direito digital	☐	☐	☐	☐	☐	☐
Políticas, planos, normas de segurança	☐	☐	☐	☐	☐	☐
Segurança da informação aplicada aos sistemas de informação	☐	☐	☐	☐	☐	☐
Outre tema	☐	☐	☐	☐	☐	☐

Especifique: _____

Descreva brevemente as principais atividades relacionadas ao seu exercício profissional.

_____

_____

PARTE 3 – BUSCA DE INFORMAÇÃO DO ESPECIALISTA

Quais são os principais CONGRESSOS e WORKSHOPS na área?

	Extremamente relevante	Relevsnte	De alguma relevância	Irrelevante	Não conheço este evento
Asiacrypt 2013	☐	☐	☐	☐	☐
Crypto 2012	☐	☐	☐	☐	☐
Cryptographic hardware and Embedded Systems (CHES 2012)	☐	☐	☐	☐	☐
Eurocrypt 2012	☐	☐	☐	☐	☐
Gartner Security & Risk Management Summit	☐	☐	☐	☐	☐
Infosec World Conference & Expo 2013	☐	☐	☐	☐	☐
20th International Workshop on Fast Software Encryption (FSE2013)	☐	☐	☐	☐	☐
Public Key Cryptography 2013	☐	☐	☐	☐	☐
RSA Conference 2013	☐	☐	☐	☐	☐

Indique um ou mais CONGRESSOS, SEMINÁRIOS e WORKSHOPS que você considera RELEVANTES.

_____

_____

_____

Para cada tipo de FONTE DE INFORMAÇÃO listado abaixo, indique a FREQUÊNCIA com que as utiliza.

	Pelo menos 1 vez por dia	Pelo menos 1 vez por semana	Pelo menos 1 vez por mês	Pelo menos 1 vez por semestre	Pelo menos 1 vez por ano	Não utilizo essa fonte
Anais de congressos	☐	☐	☐	☐	☐	☐
Congressos/workshops/cursos/eventos	☐	☐	☐	☐	☐	☐
Papers (artigos)	☐	☐	☐	☐	☐	☐
Sites de busca (Google, Yahoo, etc.)	☐	☐	☐	☐	☐	☐
Sites especializados	☐	☐	☐	☐	☐	☐
Site corporativo interno, portal interno, wiki interna, sistema interno	☐	☐	☐	☐	☐	☐
E-mail (como fonte de informação sobre S.I e Criptografia)	☐	☐	☐	☐	☐	☐
Colegas, especialistas e pesquisadores	☐	☐	☐	☐	☐	☐
Segurança da informação aplicada aos sistemas de informação	☐	☐	☐	☐	☐	☐
Revistas e livros especializados	☐	☐	☐	☐	☐	☐

Para cada tipo de FONTE DE INFORMAÇÃO, indique a RELEVÂNCIA para seu trabalho.

	Extremamente relevante	Relevante	De alguma relevância	Irrelevante	Não utilizo essa fonte
Anais de congressos	☐	☐	☐	☐	☐
Congressos/workshops/cursos/eventos	☐	☐	☐	☐	☐

Papers (artigos)	☐	☐	☐	☐	☐
Sites de busca (Google, Yahoo, etc.)	☐	☐	☐	☐	☐
Sites especializados	☐	☐	☐	☐	☐
Site corporativo interno, portal interno, wiki interna, sistema interno	☐	☐	☐	☐	☐
E-mail (como fonte de informação sobre S.I e Criptografia)	☐	☐	☐	☐	☐
Colegas, especialistas e pesquisadores	☐	☐	☐	☐	☐
Segurança da informação aplicada aos sistemas de informação	☐	☐	☐	☐	☐
Revistas e livros especializados	☐	☐	☐	☐	☐

Para cada tipo de FONTE DE INFORMAÇÃO, INDIQUE A confiabilidade desse tipo de fonte.

	Extremamente confiável	**Confiável**	**Razoavelmente confiável**	**Não confiável**	**Não utilizo essa fonte**
Anais de congressos	☐	☐	☐	☐	☐
Congressos/workshops/cursos/eventos	☐	☐	☐	☐	☐
Papers (artigos)	☐	☐	☐	☐	☐
Sites de busca (Google, Yahoo, etc.)	☐	☐	☐	☐	☐
Sites especializados	☐	☐	☐	☐	☐
Site corporativo interno, portal interno, wiki interna, sistema interno	☐	☐	☐	☐	☐
E-mail (como fonte de informação sobre S.I e Criptografia)	☐	☐	☐	☐	☐

Colegas, especialistas e pesquisadores	☐	☐	☐	☐	☐
Segurança da informação aplicada aos sistemas de informação	☐	☐	☐	☐	☐
Revistas e livros especializados	☐	☐	☐	☐	☐

Para cada site sobre SEGURANÇA DA INFORMAÇÃO e CRIPTOGRAFIA listado abaixo, indique a RELEVÂNCIA para o seu trabalho/pesquisa?

	Extremamente relevante	**Relevante**	**De alguma relevância**	**Irrelevante**	**Apenas conheço**	**Não conheço**
http://www.iacr.org - INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH	☐	☐	☐	☐	☐	☐
http://www.cert.org - SOFTWARE ENGINEERING INSTITUTE - CARNEGIE MELLON UNIVERSITY	☐	☐	☐	☐	☐	☐
http://www.cert.br - CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES	☐	☐	☐	☐	☐	☐
http://www.cve.mitre.org - COMMON VULNERABILITIES AND EXPOSURES - MIT	☐	☐	☐	☐	☐	☐
http://www.nic.br - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR	☐	☐	☐	☐	☐	☐
http://www.nvd.nist.gov - NATIONAL VULNERABILITY DATABASE - NIST	☐	☐	☐	☐	☐	☐
http://www.rnp.br - REDE NACIONAL DE ENSINO E PESQUISA - RNP	☐	☐	☐	☐	☐	☐
http://www.sans.org - SANS INSTITUTE - CRITICAL SECURITY CONTROLS	☐	☐	☐	☐	☐	☐

http://www.linuxsecurity.com/ - LINUX SECURITY	☐	☐	☐	☐	☐	☐
http://www.securityfocus.com - SYMANTEC CONNECT	☐	☐	☐	☐	☐	☐
http://www.exploit-db.com/ - THE EXPLOIT DATABASE	☐	☐	☐	☐	☐	☐
http://tools.cisco.com/security/ center/home.x	☐	☐	☐	☐	☐	☐
SECURITY INTELLIGENCE OPERATIONS	☐	☐	☐	☐	☐	☐

Indique um ou mais sites sobre SEGURANÇA DA INFORMAÇÃO e/ou CRIPTOGRAFIA que você considera RELEVANTES.

_____

_____

_____

Indique ou mais LIVROS e/ou REVISTAS/ESPECIALIZADAS que você considera RELEVANTES.

_____

_____

_____

PARTE 3 – BUSCA DE INFORMAÇÃO DO ESPECIALISTA

Indique a FREQUÊNCIA de USO DA INFORMAÇÃO para cada uma das finalidades abaixo:

	Pelo menos 1 vez por dia	**Pelo menos 1 vez por semana**	**Pelo menos 1 vez por mês**	**Pelo menos 1 vez por semestre**	**Pelo menos 1 vez por ano**	Não USO a informação para esses fins
Solução de problemas	☐	☐	☐	☐	☐	☐
Aprendizado (adquirir novos conhecimentos)	☐	☐	☐	☐	☐	☐
Compartilhamento (compartilhar as informações com outros colegas e pesquisadores)	☐	☐	☐	☐	☐	☐
Armazenamento (para uso posterior e em registros pessoais)	☐	☐	☐	☐	☐	☐

Indique a RELEVÂNCIA do USO DA INFORMAÇÃO para cada uma das finalidades abaixo:

	Extremamente relevante	**Relevante**	**De alguma relevância**	**Irrelevante**	Não USO a informação para esses fins
Solução de problemas	☐	☐	☐	☐	☐
Aprendizado (adquirir novos conhecimentos)	☐	☐	☐	☐	☐
Compartilhamento (compartilhar as informações com outros colegas e pesquisadores)	☐	☐	☐	☐	☐
Armazenamento (para uso posterior e em registros pessoais)	☐	☐	☐	☐	☐

Anexo B – Entrevista

Universidade de Brasília

COMPORTAMENTO INFORMACIONAL DE ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA

PARTE 1 - PERFIL DO PROFISSIONAL.

Nome

_____

PARTE 2 – NECESSIDADE DE INFORMAÇÃO.

Quais são as principais atividades executadas pelo especialista em Segurança da Informação e/ou Criptografia?

_____
_____
_____

Como e quando você percebe que necessita de informação?

_____
_____
_____

Essa necessidade de informação surge bem definida?

_____
_____
_____

PARTE 3 – BUSCA DE INFORMAÇÃO.

O que o motiva a buscar?

_____
_____
_____

O que o faz desistir?

_____
_____
_____

Descreva o modo com você busca a informação?

_____
_____
_____

Que tipo de informação você consulta?

_____
_____
_____

PARTE 4 – USO DE INFORMAÇÃO.

Como você utiliza a informação?

_____
_____
_____

Anexo C – RENASIC/COMSIC

A rede RENASIC foi criada em 2008, pela portaria nº 31 de 06 de outubro de 2008, com a finalidade de elevar a competência brasileira em Segurança da Informação e Criptografia (SIC) ao nível dos países mais desenvolvidos em C&T, pelo estabelecimento e efetivo aumento da integração das pesquisas brasileiras realizadas nas universidades, institutos de pesquisa, órgãos governamentais e empresas.

Entre os objetivos específicos do RENASIC estão:

1) Estabelecimento de um nível de excelência das pesquisas nacionais nas áreas de Segurança da Informação e Criptografia, por intermédio dos seguintes instrumentos:

    a) E-integração: portal colaborativo, fóruns virtuais e listas de distribuição de e-mails;

    b) Workshops, seminários e congressos para acolher as necessidades de todos os parceiros relevantes, criar consenso sobre as agendas de pesquisa integrada, apresentações científicas e sessões de interação coletiva (“*brainstorming*”);

    c) Visitas de intercâmbio entre os pesquisadores e doutorandos;

    d) Cursos de durações diversas;

    e) Concessão de bolsas de mestrado, e pós-doutorado em Universidades de excelência no país ou no estrangeiro;

    f) Desenvolvimento de uma infraestrutura comum.

2) Fortalecimento e integração das pesquisas em Segurança da Informação e Criptografia no Brasil, diminuindo a atual fragmentação das competências através da criação de uma infraestrutura de pesquisa e de sua

organização em laboratórios virtuais e, assim, estabelecer uma agenda de pesquisa e de projetos conjuntos nessas áreas.

3) Estabelecimento de Laboratórios Virtuais que visem fomentar a pesquisa entre os membros da RENASIC; cada Laboratório Virtual terá vários grupos de trabalho; esta subestrutura será reavaliada periodicamente. A rede será organizada a fim de garantir que os Laboratórios Virtuais cooperem estreitamente no sentido de atingirem os objetivos comuns.

4) Melhoria do estado da arte na teoria e prática da Segurança da Informação e Criptografia no Brasil, igualando-a aos grandes centros internacionais:

   a) Aumento de nossa compreensão dos algoritmos e protocolos existentes;

   b) Expansão das bases teóricas da Segurança da Informação e Criptografia; e

   c) Desenvolvimento de melhores algoritmos criptográficos, protocolos e implementações, obedecendo às seguintes diretrizes: alto desempenho, baixo custo, alta segurança.

5) Desenvolvimento de uma infraestrutura comum que inclui: ferramentas para a avaliação dos algoritmos de criptografia; ambientes de avaliação para hardware e software criptográficos; instrumentação física e lógica para análise de ataques secundários (“*side-channel atacks*”), suas respectivas contramedidas, além de ferramentas para avaliação dos esquemas de defesa cibernética e forense computacional.

A RENASIC, hoje vinculada ao CDCiber - Centro de Defesa Cibernética, foi criada pela Portaria Nº 31/GSIPR, de 06 de outubro de 2008, tem a seguinte estrutura inicial, que será permanentemente revista de forma a adequá-la às circunstâncias científicas e estratégicas do momento:

- Um Comitê Diretor

- Um Comitê Técnico Científico
- Oito áreas de concentração organizadas em Laboratórios Virtuais, nome atribuído em função da extensa utilização das ferramentas disponíveis da Web 2.0:

    VIRTUS – Laboratório Virtual de Técnicas Simétricas.

    ASTECA – Laboratório Virtual de Técnicas Assimétricas.

    PROTO – Laboratório Virtual em Protocolos.

    LATIM – Laboratório Virtual de Implementações.

    LAPAD – Laboratório Virtual de Processamento de Alto Desempenho.

    QUANTA – Laboratório Virtual de Computação, Informação e Criptografia Quânticas.

    LAPROJ – Laboratório Virtual de Gestão de Projetos.

- Grupos de Trabalho (GTs) no âmbito de cada Laboratório Virtual, congregando as equipes das áreas mais especializadas.
- Entidades Associadas à RENASIC por meio de convênios: governamentais ou privadas; pequenas, médias ou grandes; nacionais ou internacionais.

A Figura 4.1 a seguir ilustra a estrutura analítica da rede RENASIC.

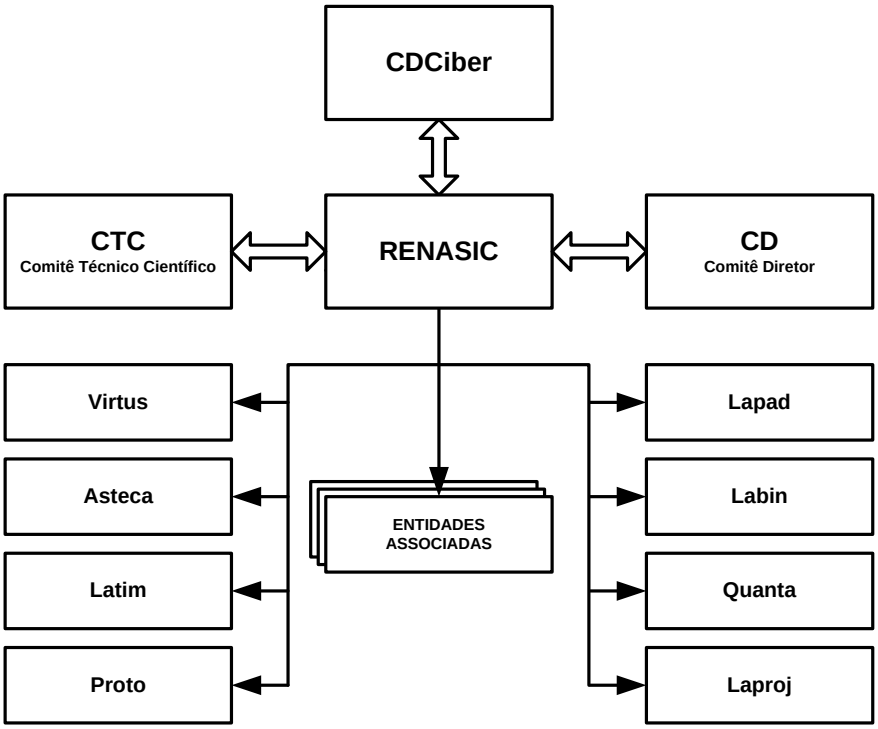

Figura 7.1 – Organograma da RENASIC

Fonte: Renasic (2008)

VIRTUS – Laboratório Virtual de Técnicas Simétricas

O Laboratório Virtual de Técnicas Simétricas enfoca todos os aspectos do desenvolvimento, análise e implementação de técnicas criptográficas simétricas e reúne as pesquisas nas seguintes áreas:

- Fundamentos teóricos das técnicas simétricas;
- Algoritmos simétricos de bloco;
- Algoritmos simétricos sequenciais;
- Códigos para autenticação de mensagens;
- Funções Hash;
- Modos de operação e uso de primitivas criptográficas simétricas.

Nessa fase inicial do VIRTUS, serão implantados apenas dois Grupos de

Trabalho cujas metas principais são as seguintes:

Identificação de padrões nos criptogramas, associando-os a elementos do sistema criptográfico que os geraram. Essa atividade é totalmente experimental. Trata-se de testar técnicas de reconhecimento de padrões ainda não utilizadas, na tentativa de obter resultados melhores dos que já foram obtidos com outras técnicas descritas em artigos. Já existe inclusive uma ferramenta de apoio aos ensaios.

Análise dos algoritmos simétricos de autenticação de SIM card do padrão GSM. Em particular, estudo e aperfeiçoamento do ataque publicado ao algoritmo "comp 128 v1", bem como a realização de um estudo heurístico das novas versões do algoritmo.

ASTECA – Laboratório Virtual de Técnicas Criptográficas Assimétricas

O ASTECA enfoca todos os aspectos da pesquisa, desenvolvimento, análise e implementação das técnicas criptográficas assimétricas e coordena as pesquisas nas seguintes áreas:

- Pesquisa de novas técnicas criptográficas assimétricas.
- Desenvolvimento e análise de algoritmos de chaves públicas.
- Segurança demonstrável.
- Assinaturas digitais.

Nessa primeira fase de implantação do ASTECA, os esforços nos temas acima mencionados serão concentrados num único projeto cujo objetivo é o incremento dos conhecimentos da comunidade criptográfica brasileira em técnicas assimétricas, o que será operacionalizado através do desenvolvimento de um projeto específico, o Assinador Cifrador Elíptico - ACE.

O ACE consiste em especificar, modelar, desenvolver e testar um sistema criptográfico assimétrico adequado ao uso em ambientes distribuídos compatível

com a ICP-Brasil. Está orientado para o melhor desempenho computacional do que os atuais sistemas disponíveis, por meio da utilização de novos modelos matemáticos para criptografia assimétrica, como curvas elípticas.

PROTO – Laboratório Virtual de Protocolos

O objetivo geral é o de implantar um laboratório de análise e desenvolvimento de protocolos seguros, permitindo a atuação de um grupo de pesquisa nessa área, em especial para execução, no período do projeto, de três esforços articulados de pesquisa referentes aos temas:

- Estudos de Soluções Técnicas e Administrativas Seguras para a Nova Geração de Sistemas de Nomes da Internet – STADS
- Sistema Criptográfico de Chave Única para uso em Redes – ScuNet
- Prospecção da viabilidade de protocolo para realização de eleições por meio da Internet (VotoNet).

Este Laboratório Virtual coordena as pesquisas para o desenvolvimento e implementação de protocolos criptográficos seguros. Esses protocolos envolvem a interação entre dois ou mais agentes, que podem ser homens ou máquinas.

Os objetivos dos protocolos - desenvolvidos e analisados contra todos os tipos de ataques - são os mais variados, por exemplo:

- Identificação segura de agentes: homem-homem; homem-máquina ou máquina-máquina;
- Métodos de pagamento eletrônico seguro;
- Intercâmbio confiável de informações;
- Votação eletrônica segura;
- Métodos de leilão seguro, e
- Contratos eletrônicos.

Este Laboratório Virtual deverá coordenar pesquisas nas seguintes áreas:

- Modelos e definições
- Protocolos seguros de computação.
- Protocolos criptográficos racionais.

O PROTO, em sua estrutura final, deverá se organizar em três grupos de trabalho:

1) GT 1 Modelos e definições, com os seguintes temas:
    - Protocolos de acordo de chaves e autenticação;
    - Provas de zero-knowledge;
    - Protocolos para identificação;
2) GT 2: Protocolos seguros de computação:
    - Computação eficiente entre múltiplas partes (MPC)
    - Segurança Demonstrável para protocolos:
    - Votação
    - Leilão e licitação eletrônica segura
    - Criptografia no limiar
    - Protocolos de acordo assíncronos;
    - Protocolos incondicionalmente seguros
3) GT 3: Protocolos criptográficos racionais:
    - Comportamento racional e modelos econômicos e de Teoria dos Jogos.
    - Computação entre múltiplos participantes racionais.

Nessa primeira fase de implantação da RENASIC por intermédio da FINEP serão buscadas as seguintes metas específicas:

1. Implantação e operação do laboratório PROTO.
2. Mecanismos de proteção de nova versão DNS - Subprotocolo de nova versão DNS.

3. Proposta de política de governo sobre sistema multilateral de domínios (DNS).
4. Subsistema de análise do protocolo para detecção de intrusão e geração de estatísticas.
5. GSC - Gerador de Sequencias Criptográficas (SCs)
6. CDSC - Centro de Distribuição de Sequências Criptográficas
7. PTSC - Protocolo de Transporte de Sequências Criptográficas
8. Coordenação e Gestão do Projeto
9. Prospecção da viabilidade de protocolo para realização de eleições por meio da Internet (VotoNet)

LATIM – Laboratório Virtual de Implantações

O LATIM (Laboratório Virtual de Implementações) possui um duplo papel no âmbito da RENASIC. Por um lado, realiza intensas pesquisas em novas técnicas relacionadas a implementações seguras. Por outro, este laboratório serve como intersecção entre as comunidades teóricas e os potenciais usuários.

Seus objetivos podem ser assim sumarizados:

- Desenvolvimento de novas e eficientes técnicas de implementação em *hardware* e *software*;
- Desenvolvimento de sólida compreensão dos ataques secundários (*side-channel attacks*) e suas respectivas contramedidas;
- Estudos e pesquisas dos *hardwares* criptoanalíticos e seus impactos nos parâmetros criptográficos.

Existem também objetivos não técnicos, tais como o incremento da cooperação entre os desenvolvedores, os engenheiros e os teóricos da criptografia, interligando as comunidades das empresas com a Academia. Pretende também realimentar os grupos teóricos com as dificuldades e problemas práticos advindos das implementações.

O LATIM é composto de cinco GTs:

GT 1: Implementações em software;

GT 2: Implementações em hardware;

GT 3: Ataques secundários.

GT 4: Avaliação de conformidade;

GT 5: Gerenciamento de Identidades.

LAPAD – Laboratório Virtual de Processamento de Alto Desempenho

A característica mais significativa do presente subprojeto é sua natureza integradora, tendo em vista que a estrutura computacional implementada na primeira fase será disponibilizada para uso de todos os Laboratórios Virtuais envolvidos no presente projeto, podendo também seu uso ser estendido à toda a comunidade científica e tecnológica relacionada com SIC.

Com o crescente aumento da conectividade entre os mais diversos dispositivos, torna-se cada vez mais necessária uma maior atenção aos mecanismos de segurança e sua eficácia, em especial para a área de criptografia. Por outro lado, os crescentes ataques cibernéticos requerem o desenvolvimento de métodos mais sofisticados de proteção da informação que, por sua vez, necessitam de uma capacidade de processamento diferenciada. Assim, a busca por métodos que mantenham a eficiência do processo de proteção da informação torna-se essencial.

A necessidade de PAD em SIC é internacionalmente reconhecida, mas não há histórico de uso significativo de PAD em SIC no país, pela inexistência, em nosso território, de máquinas suficientemente poderosas e destinadas exclusivamente para SIC e pela falta de interação entre as comunidades de PAD e de SIC.

O LAPAD visa a preencher essa lacuna, ofertando maquinário computacional poderoso e inovador, a custo acessível, que possa ser alocado exclusivamente a uma aplicação em SIC, além de serviços de consultoria em desenvolvimento e aperfeiçoamento de software para a comunidade nacional de SIC.

A inovação no maquinário computacional reside no uso de aceleradores (GPUs) em SIC. Trata-se de pesquisa inovadora. A inserção desse equipamento em máquinas existentes aumenta, potencialmente, o poderio da máquina em uma ordem de magnitude, a uma fração do custo original. A eficácia deste equipamento em diversas áreas de aplicação já é internacionalmente reconhecida (na indústria petrolífera, por exemplo). Utilizar esta tecnologia possibilita ofertar máquina poderosa para SIC a uma fração do custo de máquina equivalente sem essa tecnologia.

Entretanto, extrair desempenho de aceleradores requer codificação específica, conhecimento substancial de PAD e aplicações adequadas. Consequentemente, a atuação conjunta de especialistas em PAD com especialistas em SIC é essencial para o uso adequado do equipamento.

Por outro lado, não é necessário que a aplicação utilize eficientemente os aceleradores para que a máquina seja útil à comunidade nacional de SIC. A arquitetura da máquina proposta (Cluster de PCs acelerado por GPUs) permite seu uso sem os aceleradores. Por ser uma máquina exclusiva de SIC, pode ser reservada para testes que requeiram, por exemplo, dias de processamento com exclusividade e confidencialidade. Nesses casos, e se necessário, a máquina pode ser desconectada da Internet, fornecendo as condições de segurança necessárias para os testes, o que não pode ser garantido por máquinas de uso geral.

O sucesso deste projeto permite colimar esforços em SIC no país em torno de métodos mais seguros de comunicação, com ganhos óbvios.

LAPROJ – Laboratório Virtual de Gestão de Projetos

O LAPROJ - Laboratório Virtual de Acompanhamento de Projetos será implantado à medida que surgirem projetos originados de demandas específicas dos Associados da RENASIC, sejam entidades governamentais ou privadas.

As propostas deverão ser analisadas pelos comitês de gestão da RENASIC (CD e CTC) e, se aprovadas, devem ser objeto de planejamento detalhado.

Para cada projeto será selecionado o gerente e a equipe que participará, criando-se tópicos específicos nesta web, que aglutinarão todas as informações referentes ao respectivo projeto.