Universidade de Brasília

Faculdade de Ciência da Informação

Programa de Pós-Graduação em Ciência da Informação (PPGCINF)

Prevenção para ataques de engenharia social:
um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos

Raul Carvalho de Souza

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 Henrique Cabral Fernandes

Brasília, 16 de junho de 2015

Souza, Raul Carvalho de

Prevenção para ataques de engenharia social: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos / Raul Carvalho de Souza - Brasília, DF, 2015.
200 p.

Orientador: Prof. Dr. Jorge Henrique Cabral Fernandes

Dissertação (mestrado) - Universidade de Brasília - UnB. Programa de Pós-Graduação em Ciência da Informação.

Bibliografia: p. 153 – 159.

1. Ciência da Informação. 2. Confiança. 3. Risco. 4. Segurança da Informação. 5. Análise de Redes Sociais.

I. Fernandes, Jorge Henrique Cabral. II. Universidade de Brasília - UnB. Programa de Pós-Graduação em Ciência da Informação. III. Título

CDU 005.31:519.1:004.9

FOLHA DE APROVAÇÃO

Título: "PREVENÇÃO PARA ATAQUES DE ENGENHARIA SOCIAL: UM ESTUDO SOBRE A CONFIANÇA EM SEGURANÇA DA INFORMAÇÃO EM UMA ÓTICA OBJETIVA, SOCIAL, ESTRUTURAL E INTERDISCIPLINAR UTILIZANDO FONTES DE DADOS ABERTOS."

Autor (a): Raul Carvalho de Souza

Área de concentração: Gestão da Informação

Linha de pesquisa: Comunicação e Mediação 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.

Brasília, 07 de agosto de 2015.

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

Prof. Dr. Roberto Wagner da Silva Rodrigues
Membro Titular (MDA)

Profª. Drª. Ivette Kafure Muñoz
Membro Titular (UnB/PPGCINF)

Profª. Drª. Dulce Maria Baptista
Membro Suplente (UnB/PPGCINF)

Este trabalho é dedicado a Deus, por ter criado tudo e ainda possibilitar que contemplemos esse mundo perfeito por natureza e imperfeito por necessidade humana. Apreciamos essas maravilhas de Sua criação pelo poder do conhecimento e desejamos um dia na Sua imagem e semelhança copiar humildemente Sua obra no que julgamos justiça e conforto para todos.

Agradecimento

Agradeço a minha esposa, Brenda, por me apoiar nas dificuldades. Aos meus familiares, muito obrigado pelo suporte incondicional. Agradeço ao meu orientador, dr. Jorge Fernandes, por aceitar ser meu orientador no programa e no grupo de pesquisa. Obrigado aos professores Leonardo Lazarte e Blanca Lazarte pelas instruções acadêmicas e pela amizade. Ao Msc. Ricardo Sampaio, à Msc. Helena Sacerdote, ao Msc. Rafael Henrique, ao Msc. Robson e, não menos importante, colega de luta pela aprovação no Mestrado, Alcimar Rangel, colegas de grupo de pesquisa, obrigado.

Agradeço aos professores Ivette Kafure e Roberto Wagner pelas revisões, pelas críticas e pelos exames no relatório intermediário. Agradeço à servidora Martha e demais servidores da Secretaria e da Coordenação do curso pelo apoio administrativo na faculdade e na universidade. Agradeço a Yana Palankof pelas revisões no texto.

Agradeço aos chefes onde trabalho, que me autorizaram a frequentar as aulas. Agradeço aos colegas de trabalho que na minha ausência executaram nossas atividades e mantiveram o estado das coisas o mais tranquilo possível.

“O único lugar aonde o sucesso vem antes do trabalho
é no dicionário.”
Albert Einstein

“Os bons vi sempre passar
No mundo graves tormentos;
E para mais me espantar,
Os maus vi sempre nadar
Em mar de contentamentos...”
Luís Vaz de Camões.

“Só um sentido de invenção e uma necessidade intensa de criar
levam o homem a revoltar-se,
a descobrir e a descobrir-se com lucidez.”
Pablo Picasso

“Se as coisas são inatingíveis... ora!
Não é motivo para não querê-las...
Que tristes os caminhos, se não fora
A presença distante das estrelas!”
Mario Quintana

“Nunca te orgulhes de haver vencido um adversário,
o que venceste hoje poderá derrotar-te amanhã.
A única vitória que perdura é
a que se conquista sobre a própria ignorância.”
Jigoro Kano

“Somente se aproxima da perfeição
quem a procura com constância,
sabedoria e, sobretudo
humildade.”
Jigoro Kano

“Enquanto a cor da pele for mais importante que o brilho dos olhos,
haverá guerra.”
Bob Marley

“A língua dos sábios torna o ensino interessante,
mas a boca dos insensatos é fonte de tolices.
Os olhos do SENHOR estão em toda parte:
Ele observa atentamente os maus e os bons! ”
Provérbios, 15:2,3

RESUMO

Há um embate sobre os aspectos objetivos e os aspectos subjetivos no estabelecimento da confiança interpessoal organizacional. Na contemporaneidade, esse embate gera riscos na segurança da informação (SI) e na segurança cibernética. Este estudo procura demonstrar que o espaço informacional está constantemente ameaçado, em risco de violação das propriedades básicas da segurança da informação. Trata também do abuso da confiança como plausível causa do fracasso de algum projeto organizacional, ou mesmo do malogro da organização por completo, devido à violação das propriedades básicas da segurança da informação. Ao mesmo tempo, a pesquisa investiga definições práticas a respeito da confiança e do risco e foi feita com o auxílio da análise de redes sociais (ARS) e da computação, em uma abordagem interdisciplinar da Ciência da Informação (CI) e métodos para análise de vulnerabilidades em engenharia social. Aqui se defende que os profissionais da segurança da informação da atualidade devem formar-se na área da CI, pois poderiam, com esse conhecimento interdisciplinar, utilizando a ARS, estudar modelos de comportamento informacional nas organizações e nas empresas. Assim, poderiam ser identificados e analisados os fluxos de informações e as comunicações. Desse modo, seria possível a identificação de alguns aspectos objetivos em estruturas sociais por meio da observação, de modo exploratório, de uma nova inteligência, necessária para os assuntos de segurança. A engenharia social é considerada uma das grandes ameaças a serem enfrentadas na segurança da informação, principalmente por que é focada no fator humano. O fator humano pode ser o elemento mais resiliente da segurança, mas pode ser explorado tendo-se em vista suas carências e necessidades. A engenharia social alavanca a confiança nos relacionamentos interpessoais para obter vantagens indevidas. Dessa forma, esta dissertação tenta responder à seguinte questão: como podem ser identificados alvos para ataques de engenharia social no que se refere ao abuso de confiança se utilizando como ferramenta a ARS aplicada em dados abertos?

Palavras-chave: Confiança. Risco. Segurança da informação.

ABSTRACT

This work demonstrates that there is a challenge on the objective and subjective aspects in establishing the organizational interpersonal trust. This conjectural collision generates risks in information security (IS) and cyber security, nowadays. This study seeks to demonstrate that the information space is constantly threatened, at risk of violation of the basic information security properties. Shows the abuse of trust as plausible cause of the failure of some organizational project, or even the failure of the organization altogether, for breach of the basic information security properties. Investigates objective definitions regarding trust and risk. Research, with the help of social network analysis (SNA), with the help of computing, in an interdisciplinary approach of Information Science (ISc) methods for analysis of vulnerabilities in Social Engineering. Argues that today's information security professionals should be formed in the area of ISc. This security professionals may use this interdisciplinary knowledge to study, with SNA, this information's behavior's models of organizations and businesses. So, may identificaty and analyses communication and information flows. Thus, it would be possible to identify some objective aspects in social structures, through observation, in a exploratory way, in a new intelligence necessary for security issues. Social engineering is considered one of the greatest threats to be faced in information security, mainly because it is focused on the human factor. The human factor can be the most resilient element of security, but it can be explored from your wants and needs. The Social Engineering lever the interpersonal relationships trust for undue advantage. Thus, this dissertation attempts to answer the question of how may be identified as social engineering's targets attack, in regard to trust abuse, with SNA as a tool applied in open data.

Keywords: Trust. Risk. Information security.

Lista de figuras

Figura 1. Um grafo (pode representar um sociograma) 24
Figura 2. Pergunta principal e perguntas auxiliares da pesquisa 26
Figura 3. Portal da Transparência 31
Figura 4. Processo metodológico 33
Figura 5. Modelo Entidade Relacionamento 38
Figura 6. Modelo de solução tecnológica 38
Figura 7. Captura de tela com máquinas virtuais executando scripts de coleta 39
Figura 8. Captura de tela com máquinas virtuais executando scripts de coleta e banco de dados 39
Figura 9. Os mundos de Popper 47
Figura 10. Relação entre dado, informação, conhecimento e mensagem 50
Figura 11. Elementos da arquitetura da informação (AI) 51
Figura 12. Fórmula de Lasswell em modo gráfico 57
Figura 13. Extensão da fórmula de Lasswell proposta por Braddock 57
Figura 14. Modelo de Shannon 58
Figura 15. Modelo helicoidal de Dance 58
Figura 16. Modelo de De Fleur, inspirado em Shannon e Weaver, adicionando feedback 59
Figura 17. Modelo transacional de Tubbs 60
Figura 18. Informational link 62
Figura 19. Rede com vários fluxos de informação 62
Figura 20. Modelo do perde-e-ganha entre segurança, da funcionalide e da utilidade 67
Figura 21. Disposição dos conflitos de interesse sobre um indivíduo 74
Figura 22. Pirâmide de seleção do alvo 76
Figura 23. Mapa conceitual entre sociedade, dilemas sociais e pressões sociais 77
Figura 24. Framework de engenharia social 85
Figura 25. Menu principal do ToolKit SET (Social Engeneer Toolkit) 96
Figura 26. Grafo dirigido 100
Figura 27. Grafo não dirigido 100
Figura 28. Mercado de manufatura de metais e partições (clusters) 101
Figura 29. Uma pessoa, outro e X (coisa) 104

Figura 30. Grafo balanceado 104
Figura 31. Papéis de corretagem em uma rede social 105
Figura 32. Tela principal do Pajek 107
Figura 33. Tela de visualização do Pajek 108
Figura 34. Arquivo de uma rede no Pajek..... 108
Figura 35. Criando clusters no Pajek..... 109
Figura 36. Realizando uma transformação no Pajek..... 110
Figura 37. Extração no Pajek..... 110
Figura 38. Grafo com pesos discretos (sociograma) 116
Figura 39. Grafo com pesos probabilísticos (sociograma)..... 116
Figura 40. Distância emocional..... 118
Figura 41. Sociograma da extração do Portal da Transparência..... 123
Figura 42. Rede extraída e com primeira transformação..... 124
Figura 43. Organização dos componentes, segunda transformação..... 124
Figura 44. Componentes com mais de dois vértices destacados..... 125
Figura 45. Extração dos componentes com mais de dois vértices 125
Figura 46. Componentes apresentados com partição de UG/favorecido..... 126
Figura 47. Componentes marcados com o valor do cluster ao qual pertencem 127
Figura 48. Componente 18 – um caso para ser explorado..... 127
Figura 49. Rede contendo apenas registros coletados em 2014..... 128
Figura 50. Rede organizada em componentes isomorfos..... 129
Figura 51. Criação de partição com componentes maiores que dois nós..... 129
Figura 52. Isolados quatro componentes para análise 130
Figura 53. Apresentação de rótulos para cada nó 130
Figura 54. Recorte de quatro componentes para análise 132
Figura 55. Percentual sobre prestatividade própria 133
Figura 56. Percentual sobre a importância da prestatividade 133
Figura 57. Percentual sobre prestatividade aos terceirizados 133
Figura 58. Percentual de delegação de tarefas remotamente 134
Figura 59. Percentural de tarefas executadas remotamente por terceiros 134
Figura 60. Percentual de pessoas que tiveram equipamentos acessados remotamente 134
Figura 61. Percentual de pessoas que conhecem ou não quem acessa seus equipamentos remotamente 135

Figura 62. Percentual de trabalhos realizados remotamente.....135
Figura 63. Percentual de confiança nos fornecedores.....135
Figura 64. Percentual de conhecimento sobre senhas enviadas por mensagem.....136
Figura 65. Percentual dos que recebem ou não listas de funcionários prestadores de serviço 136
Figura 66. Percentual de pessoas que trabalham com protocolos laborais com terceiros 136
Figura 67. Percentual dos que conhecem ou não a classificação da informação.....137
Figura 68. Percentual dos que já classificaram informação.....137
Figura 69. Percentual dos que conhecem ou não engenharia social 137
Figura 70. Tríade Estado-Maior e contratadas 142
Figura 71. Tríade Casa da Moeda e contratadas 142
Figura 72. Tríade PMDF e Antaq.....144
Figura 73. Componente com universidades 146
Figura 74. Relação entre autorização, informação e propriedades básicas da segurança da informação.....148
Figura 75. Relação entre autorização e confiança.....149
Figura 76. Mapa conceitual do referencial teórico 155
Figura 77. Relação entre a base da segurança da informação e a confiança 158
Figura 78. Modelo de uma possível implementação de sistema de controle para intervenção preemptiva, proativa.....163

Lista de tabelas

Tabela 1. Necessidades e funcionalidades.....37
Tabela 2. Organizações nas quais trabalham os servidores consultados 40
Tabela 3. Opiniões dos consultados, mascaradas 139

Lista de siglas

APA – ataques persistentes avançados
ARS – análise de redes sociais
CI – Ciência da Informação
IC – *Information Science* (Ciência da Informação)
ES – engenharia social
EngS – engenheiro social
PDCA – *plan do check act* (planejar, realizar, controlar, agir)
PGDF – Procuradoria-Geral do Distrito Federal
Serpro – Serviço Federal de Processamento de Dados
SI – segurança da informação
SIC – segurança da informação e comunicações
SNA – *social network analysis* (análise de redes sociais)
TOR – rede de computadores anônima da internet
TI – tecnologia da informação

Sumário

1 Introdução 16
2 O projeto da pesquisa 20
2.1 Justificativa 20
2.2 A questão da pesquisa 25
2.3 Objetivos 27
2.4 Metodologia 28
2.4.1 Metodologia da coleta de dados 34
2.4.2 Pesquisa de opinião com servidores públicos 40
3 Fundamentos conceituais 43
3.1 A ciência da informação e a informação 43
3.2 Comunicação e mediação da informação 55
3.3 Segurança – ataque, alvo, vulnerabilidade – e a gestão de riscos da informação 63
3.4 Engenharia social 79
3.4.1 Ferramentas de engenharia social 93
3.5 Fundamentos da análise de redes sociais 98
3.5.1 Análise de redes sociais (ARS) 98
3.5.2 O *software* Pajek 107
3.5.3 Confiança e risco 112
3.5.4 Confiança 112
3.5.5 Risco 119
4 Resultados 122
4.1 Análise dos dados e discussão 122
4.1.1 Primeira bateria de coletas dos dados 122
4.1.2 Segunda bateria de análise dos dados 127
4.1.3 Resultado da pesquisa de opinião 132
4.1.4 Discussão 140
4.2 Conclusão 151
4.3 Limitações 160
4.4 Trabalhos futuros 161
Referências 164

5 Glossário.....171
Apêndice A – Questionário da pesquisa de opinião 173
Apêndice B – Trechos do código fonte da carga de dados 176
Apêndice C – Trechos do código fonte do coletor de dados 179
Apêndice D – Trechos do código fonte criador de rede para o Pajek.....187

1 Introdução

Determinar objetivamente[1] aspectos sobre a confiança e o risco no tema segurança da informação (SI) e segurança cibernética[2] é um desafio complexo e contemporâneo. Como estudar esse fenômeno é, atualmente, uma incógnita na ciência. A suspeita é que seria preciso utilizar conhecimentos de várias disciplinas para estudá-lo, até porque há necessidade de entender o que são a informação, a segurança, os aspectos objetivos e comportamentais nas relações interpessoais, entre outros conceitos, em um mesmo contexto, para encontrar respostas para tais desafios da SI.

Zins (2007) defende que os diferentes domínios de conhecimento implicam diferentes campos de estudo na Ciência da Informação (CI), tornando-a uma matéria interdisciplinar. Saracevic (1995) também defende a interdisciplinaridade da Ciência da Informação. Assim, ao se buscar respostas para problemas sociais ligados aos ataques de segurança da informação seria importante utilizar a CI considerando alguns conceitos da sociologia, da ciência da computação, da ciência jurídica e da psicologia. Provavelmente por isso Fernandes (2010d) afiança a necessidade de os profissionais da segurança da informação se capacitarem em CI. O autor afirma que os trabalhadores responsáveis pela segurança da informação possuem, hoje, formação técnica, apresentando-se ainda em estágio de amadurecimento quanto ao melhor emprego de suas habilidades. Conforme Fernandes, tais trabalhadores devem ser formados na área da Ciência da Informação, pois precisam entender o contexto social, ético, cultural e legal para poder solucionar alguns problemas de segurança da informação nas organizações.

Segundo Saracevic (1995), a Ciência da Informação tem uma forte dimensão social e humana. Silva et al. (2005) informam que a análise de redes sociais (ARS) pode ser

[1] Silva (2006) explica que o substantivo “objetivo” é derivado do verbo latino *objecere* (pôr diante, apresentar); literalmente, o vocábulo exprime tudo o que é visível, concreto, real, positivo, em oposição ao termo “subjetividade”, que se refere ao sujeito.

[2] Segundo Fernandes (2012), o termo “cibernética” é discutido por Wiener em 1948. Ele debate o trabalho de Wiener, que apresentou vários ensaios a respeito do estudo de **fenômenos de controle**, identificados por meio da análise do comportamento do sistema nervoso, de sistemas mecânicos, fenômenos psíquicos, máquinas computacionais, sistemas autorreplicantes, sociedades humanas e animais. Para Fernandes, a investigação de fenômenos de **controle, monitoramento, *feedback* e autorregulação** foi disseminada no trabalho de Wiener, que cunhou o termo cibernética.

utilizada para identificar e analisar fluxos de informações no campo da CI em organizações[3] e empresas.

Everton (2013) afirma que a ARS pode estudar a condução e a difusão de vários tipos de benesses materiais e não materiais na rede social, tais como informações e confiança, entre outros. Os métodos de análise de redes sociais são úteis quando se está interessado em investigar o comportamento das relações sociais com base na estrutura de uma rede social. Desses métodos fazem parte técnicas que promovem precisão e definição formal para os estudos sociais.

Entretanto, acredita-se que não é só no formalismo que residem as respostas para os problemas de segurança da informação. Shostack e Stewart (2008, p. 49) afirmam:

> Se considerarmos os desafios que encaramos dentro da segurança da informação como sendo problemas de lógica, as respostas para esses desafios deveriam ser encontradas através da aplicação pura da matemática. Essas hipóteses não são verdadeiras para a maioria dos profissionais de segurança. Eles entendem que os usuários e outros fatores *soft* são as razões pelas quais a segurança geralmente falha.

Assim, a solução de problemas relacionados ao comportamento de atores no espaço cibernético exige que se investiguem em diversos autores de ciências distintas conceitos que possibilitem um entendimento e uma anuência. Nesses diferenciados nichos científicos, novas óticas sobre as organizações sociais precisam ser destacadas para auxiliar a SI, talvez por meio de uma visão estrutural e comportamental dos indivíduos dessas organizações sociais. Em relação a modelos de comportamento social obrigatório, o jurista Reale (2000, p. 186) assevera:

> Hoje em dia, quando as ciências, desde a Matemática e a Cibernética até a Física e a Sociologia, falam tanto em “modelo”, como instrumento do conhecimento científico, não é demais lembrar a precedência cronológica da Ciência do Direito, a primeira a empregar “tipificações sociais”, isto é, *modelos de comportamentos obrigatório*s.

Os ditos modelos[4] de comportamento obrigatório, definidos por Reale, pensados no

[3] Uma organização, segundo a Teoria Clássica explicada em Chiavenato (2003), é uma estrutura hierárquica em uma divisão do trabalho especializado.

[4] Modelos são simplificadores, pragmáticos, sintéticos, visuais, ordenados e, além disso, são métodos. Os modelos são orientados à utilidade, são resumos executivos de relações complexas, explicam com imagem aquilo que é difícil de expressar com palavras, estruturam e não oferecem respostas – o modelo sugere as respostas. Quando precisamos dar ordem ao caos que nossa realidade complexa nos apresenta utilizamos modelos. Os modelos ajudam-nos a reduzir a complexidade, a suprimir partes para podermos nos concentrar no que realmente interessa (KROGERUS; TSCHÄPPELER, 2011).

contexto da segurança da informação, merecem atenção, pois são materializados, geralmente, em normas internacionais, leis, políticas, instruções normativas, normas complementares, manuais de boas práticas, processos organizacionais, protocolos de segurança, fluxos de trabalhos, entre outros. Quando tais modelos são criados, vislumbra-se uma sociedade justa, ou uma organização sadia, ou mesmo relações bilaterais sociais salutares.

Os modelos de comportamento obrigatório de Reale para o *hacker*[5] são obstáculos para esses objetivos. De acordo com Mäkinem (2005), a segurança, sobretudo, cria condições para a existência de atividades sociais de grande escala no tempo e no espaço. Uma sociedade em constante evolução terá sempre de aprimorar seus modelos de comportamento obrigatório.

Castelfranchi e Falcone (2001) informam haver uma tendência para o surgimento de técnicas de detecção e prevenção de fraudes que levam em consideração a confiança estabelecida nos ambientes com redes eletrônicas.

Um dos problemas da SI é a engenharia social (ES). Segundo Mitnick e Simon (2002), esta se utiliza do abuso da confiança para chegar a seus fins. A ES está se tornando uma preocupação cada dia mais forte, tendo em vista que os ataques à SI estão ficando cada vez mais avançados e complexos. Atualmente, os ataques estão combinando diversas técnicas para atingir seus objetivos. Um exemplo disso são os ataques persistentes avançados (APA), que utilizam, em muitos casos, a engenharia social como um dos vetores.

Portanto, muito provavelmente, definições objetivas sobre confiança e risco podem ser descobertas com o auxílio da ARS, da computação e de outros conceitos de outras disciplinas. Assim, esta dissertação poderia utilizar uma abordagem interdisciplinar da CI em uma proposta de verificar aspectos objetivos sobre confiança e engenharia social e, ao mesmo tempo, realizar estudos comportamentais, contribuindo para o campo do controle de uma estrutura social que promova *insights* e recomendações para a segurança da informação. Hoje, na sociedade da informação, os meios das relações sociais mudaram e, portanto, as formas de se estabelecer acordos.

Lazarte (2000) chancela a existência de novos desafios nesse mundo novo: “Além da dimensão econômica e suas implicações, **a sociedade da informação** traz mudanças

[5] O *hacker*, segundo Bill e Klein (2010), quebra as regras que ele julga estúpidas para chegar a resultados que ele julga melhores, mais espertos, mais inteligentes. Schneier (2012) doutrina que o *outlier* – podemos entender o *hacker* – é aquele que não aceita as pressões sociais e age de acordo com seus ideais, seu desejo, sua conveniência e seu egoísmo.

na forma em que interpretamos o mundo, impacta nosso ambiente interior e **põe novos desafios a nossas relações sociais** (grifo nosso)". Para Schneier (2012), a tecnologia mudou a forma com que nossas interações sociais ocorrem, mas, segundo ele, é muito fácil esquecer-se disso!

2 O projeto da pesquisa

2.1 Justificativa

A segurança da informação e a segurança cibernática estão sujeitas a dificuldades de controle devido ao ambiente no qual estão inseridas, por exemplo, as organizações e a internet. Para agravar as dificuldades, alguns conceitos, como informação e confiança, ainda não possuem uma definição unificada. Aliado a isso, a importância dos aspectos objetivos *versus* a dos aspectos subjetivos para a solução de problemas no tema é bastante controversa. Alguns defendem que os problemas de segurança podem ser resolvidos puramente com matemática, e outros apregoam que o subjeito é o "elo mais fraco", portanto estudar os aspectos subjetivos seria a solução.

Mäkinem (2005) expõe que o controle e o monitoramento são parte da segurança. Estes integram o sistema administrativo social e são baseados no armazenamento de relevantes informações sobre a conduta das pessoas. O controle e o monitoramento são necessários para se garantir o estado das coisas. A supervisão direta de conduta é parte do controle, e sem supervisão não há qualidade nos processos. Entretanto, parece perigoso permitir a qualquer um o controle e o monitoramento das informações sobre as relações sociais.

A facilidade de obtenção dos dados na internet – a rede mundial de computadores – é uma vantagem para o controle com dados abertos.[6] Eles são livres para uso, assim qualquer um pode tirar proveito, inclusive as pessoas mal intencionadas. Essa é outra razão para se proteger informações provenientes dessa categoria de dados.

A internet é um ambiente aberto, e por isso mesmo seu controle é complicado. Mäkinen (2005) assevera que a internet é uma rede caótica. As pessoas participam das atividades das redes caóticas e não têm ideia do tipo de controle a que as informações são submetidas. Essas informações podem ser usadas para interesses comerciais e controle de opinião, entre outras finalidades.

É preciso ter em mente que o espaço informacional está constantemente ameaçado, em risco de violação das características básicas de segurança da informação (ABNT, 2006). A segurança da informação, em senso comum, é o que garante a disponibilidade, a

[6] O Projeto Dados Abertos (do inglês *Project Open Data)* está registrado no *creative commons*. O Open Data (2013) afirma que "dados abertos são dados que qualquer um é livre para usar, reutilizar e redistribuir sem restrição (exceto, talvez, os requisitos de propriedade e compartilhamento)*"* (tradução nossa).

integridade e a confidencialidade nos sistemas de informação. Segundo a ABNT (2006), o sistema de segurança da informação prevê o controle como uma das etapas do ciclo P-D-C-A, a fase **C** é denominada controle (do inglês *check)*.

Acredita-se que por meio de mecanismos objetivos, obtidos por intermédio de estudos sistemáticos, no propósito de encontrar mecanismos que cessem certos comportamentos danosos ou maliciosos, com o uso de controles e contramedidas bem definidos, pode-se garantir a segurança das informações nas relações organizacionais da sociedade da informação (SOUZA, 2011).

Shostack e Stewart (2008) afiançam que o mercado de segurança da informação não trabalha tão objetivamente quanto carece. Segundo os autores, na maior parte dos casos adotam-se recomendações de fabricantes, entendendo que estas são a “melhor escolha”. Essas recomendações geralmente resultam em aquisição de algum produto. É claro que o mercado deve ser “ouvido” na busca por soluções dos problemas organizacionais e das empresas. Entretanto, ele não deve ser considerado a fonte de informação principal, tampouco a única.

A subjetividade na tomada de decisão organizacional parece um sinônimo de incerteza, e esta não é bem-vinda, pois se tem demonstrado um obstáculo na solução de alguns problemas. Esses problemas estão relacionados às ameaças ligadas à ruptura para fim torpe das características básicas da segurança da informação: disponibilidade, integridade e confidencialidade da informação.

Por sua vez, De Lazarte (2004) defende que as questões relativas à segurança digital provêm da mistura de problemas técnicos e problemas sociais. Para a autora, o aumento do uso do sistema de informação na sociedade requer maior segurança aos sistemas, de tal modo que possa dar proteção, validade e segurança jurídica aos contratos e aos compromissos assumidos por meios digitais. De Lazarte afirma que o pagamento eletrônico tem sido muito utilizado, e a criptografia é usada como ferramenta que proporciona algumas garantias e promove credibilidade nas transações. Ela alega que essas atividades baseiam-se em princípios de segurança, confiança e eficiência.

Shostack e Stewart (2008) asseguram que muitos problemas na segurança da informação são proveitosamente iluminados pela matemática e pela lógica, porém, uma vez resolvidos, surgem questões quando computadores, normas sociais e o comportamento de pessoas se cruzam.

É preciso perceber a segurança da informação como um processo, e não como um

produto (SCHNEIER, 1998). Portanto, é necessário entender os papéis do fator humano na SI. O contexto no qual os problemas deste trabalho se inserem é complexo, demanda objetividade nas ações e entendimento dos aspectos subjetivos e comportamentais dos usuários.

Há um embate dialético e o desafio de se encontrar soluções justamente no cruzamento dos aspectos objetivos e dos aspectos subjetivos, por exemplo: criptografia, credibilidade, sistemas de informação e confiança, tudo isso em uma mesma solução. É difícil assumir um lado nessa luta conjectural de objetividade *versus* subjetividade para solução dos problemas de SI.

Souza (2011) afirma que a confiança é um componente estratégico no contexto da segurança da informação. Schneier (2012) garante que a segurança é um mecanismo para sustentar um estado de confiança benéfico em grande escala, isso para que a sociedade se desenvolva. Mas, segundo o autor, sempre haverá aqueles que desejam burlar as regras de segurança para otimizar seus ganhos nas relações sociais, por exemplo, o *hacker*.

Transportando os modelos de comportamento obrigatórios de Reale para o que ensina Schneier (2012), esses referidos modelos agem como pressões sociais para criar mecanismos de confiabilidade. Para o autor, a confiança é um elemento fundamental para a sociedade. Fatalmente precisamos confiar alguns dados, informações ou conhecimentos a terceiros nos negócios organizacionais. Porém, é preciso saber que estamos confiando um dos bens organizacionais mais valiosos desta época: a sociedade da informação.

Segundo Schneier (2012), a confiança pode ser construída – aqui entendemos arquitetada – por meio de estruturas sociais. A moral, a reputação, as pressões institucionais e a segurança podem ser utilizadas para arquitetar um estado de confiança em um contexto. Fukuyama (2000) argumenta que a confiança está intimamente ligada ao capital social e é determinada pela *performance* de uma instituição social. Para ele, a confiança é determinada de forma exógena, ou seja, de fora para dentro da pessoa.

Fernandes (2012) defende a construção de um arsenal analítico para aprimorar a segurança do Estado. Acredita-se que uma forma de controlar as relações de confiança é por meio da inspeção das estruturas sociais – os sociogramas. Wasserman et al. (2009) esclarecem que sociograma é uma figura no qual as pessoas (ou, mais genericamente, qualquer unidade social) estão representadas como pontos em um espaço bidimensional, e os relacionamentos entre os pares de pessoas estão representados por linhas que ligam os correspondentes pontos.

Percebe-se que é possível sistematizar as abordagens de análise de segurança com o uso da ARS. Entende-se que a transformação das informações com o uso de sociogramas é interessante em diversos aspectos da segurança da informação, melhorando a visualização de certos problemas e possibilitando melhores *insights*, o que facilita a solução dos problemas.

A análise de redes sociais traz aspectos objetivos para identificar estruturas sociais por meio da observação da realidade. Ressler (2006) defende que a prática da ARS é a nova inteligência necessária para os assuntos de segurança. Com a ARS pode-se avaliar relacionamentos sociais entre indivíduos de forma que se identifiquem papéis e comportamentos ao longo do tempo.

É possível verificar computacionalmente o comportamento das relações sociais de um indivíduo ou grupo organizacional (DE NOOY; MRVAR; BATAGELJ, 2011). Os sociogramas, que são modelos de redes sociais, podem ser estudados por meio de termos e conceitos ou processos relacionais, que geralmente podem ser modelados matematicamente (WASSERMANN; FAUST, 1994).

Uma das representações para os sociogramas utilizadas na análise de redes sociais é o grafo. Gersting (2001) define grafo como um conjunto não vazio de nós (vértices) e um conjunto de arcos (arestas) tais que cada arco conecta dois nós. Vejamos a Figura 1 onde os nós (vértices) são representados pelas bolas numeradas e os arcos (arestas) representados pelas linhas.

Segundo Mitnick e Simon (2002), um ataque de engenharia social é uma ação elaborada, arquitetada, que explora o altruísmo e a boa vontade das pessoas. Para os autores, a engenharia social coloca o atacante em uma posição privilegiada dentro do fluxo da informação, de forma ao trapaceiro alcançar seus objetivos.

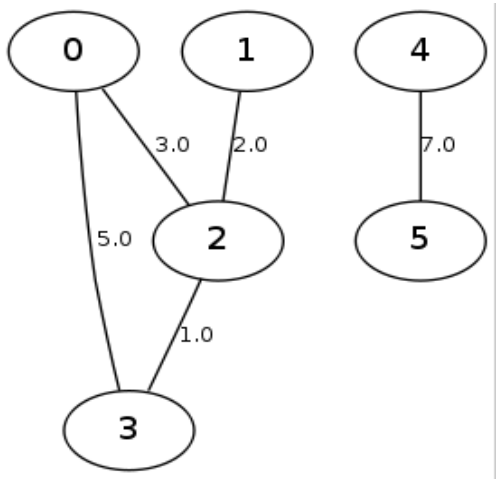


Figura 1. Um grafo (pode representar um sociograma)

Fonte: elaboração do autor

Para que os modelos de comportamento tenham sucesso e sejam ajustados é preciso que haja controle sobre as relações sociais bem como a revisão desses modelos, afinal a sociedade é dinâmica, e o monitoramento pode ser o meio a promover o entendimento das mudanças para que os ajustes possam ser recomendados. Provavelmente os golpes aplicados hoje com a ES sejam apenas variações dos mesmos golpes praticados há muito tempo.

Portanto, sugere-se a criação de metodologias que apliquem tanto conceitos de lógica quanto estudos que considerem o ponto de vista do sujeito. Por isso, justifica-se procurar entender os processos de atribuição de confiança e riscos comportamentais no tema segurança da informação, considerando seus aspectos objetivos e possivelmente apresentando *insights* para facilitar a proteção contra ataques.

Cada vez mais informações trafegam e são manipuladas de maneira instantânea, principalmente pela internet, e os detalhes técnicos ficam dia a dia mais transparentes ao usuário e aos analistas. Ações e comunicações humanas erradas usando a tecnologia da informação (TI) podem gerar grandes prejuízos para uma organização. Schneier (2003) afirma que quanto mais algo é importante para a coletividade, maior é a probabilidade de ele ser atacado.

2.2 A questão da pesquisa

É intrigante a quantidade de dados e informações oriundos das relações sociais que circula no espaço informacional e no espaço cibernético. Acredita-se que o controle sobre esse fluxo pode ser aprimorado com o uso de métodos analíticos.

O que se pode explorar de dados abertos nesse cenário de complexidade e caos é um desafio para o controle e para a segurança da informação. A engenharia social aproveita-se do caos e da desordem para obter privilégios e enganar as pessoas bem-intencionadas. A SI não é um assunto ligado puramente à tecnologia – a proteção contra ataques de engenharia social é matéria interdisciplinar. O que se pretende encontrar nesta pesquisa, a princípio, são alguns métodos de mapeamento das relações de confiança e dos riscos associados para responder à seguinte questão: como podem ser identificados os alvos de ataques de engenharia social no que se refere ao abuso de confiança, utilizando como ferramenta a análise de redes sociais aplicada em dados abertos da administração pública?

Acredita-se que para responder a essa pergunta principal é preciso responder a algumas perguntas auxiliares. Na **Figura *2*** são apresentadas perguntas auxiliares que serão usadas como suporte para alcançar os objetivos da pesquisa.

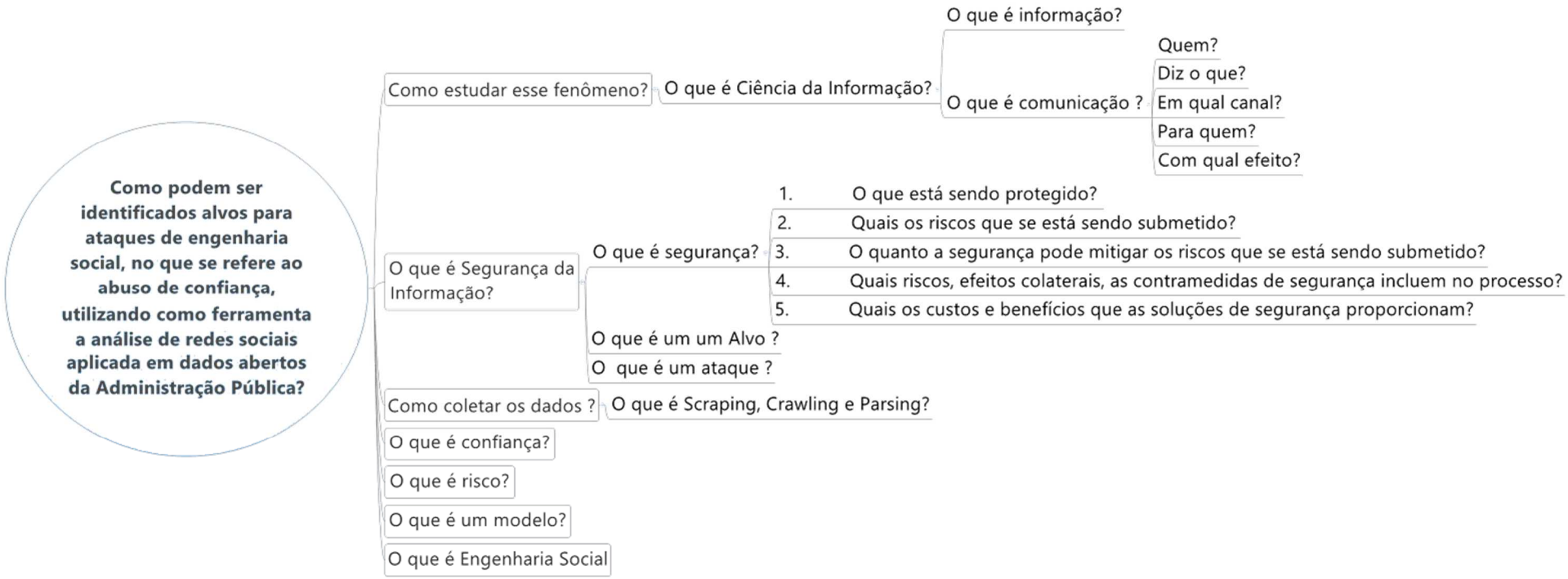


Figura 2. Pergunta principal e perguntas auxiliares da pesquisa

Fonte: elaboração do autor

2.3 Objetivos

2.3.1 Objetivo geral

Análise de redes sociais e estudo de caso para encontrar possíveis alvos de ataques de engenharia social a fim de realizar a mediação – intermediação – da comunicação com o intuito de obter *insights* e recomendações para a segurança da informação.

2.3.2 Objetivos específicos

1. Descrever como coletar e explorar os dados do Portal da Transparência, os transformando em sociogramas para Análise Estrutural e Identificação de Padrões.
2. Correlacionar Cenários e Casos de ataques de engenharia social às estruturas sociais encontradas em dados de compras em Tecnologia da Informação para identificar possíveis alvos para a engenharia social.
3. Identificar o perfil das pessoas expostas à engenharia social na Administração Pública por meio de uma pesquisa de opinião.

2.4 Metodologia

Segundo Kothari (2004), a pesquisa pode ser aplicada (ação) ou fundamental (a básica ou pura). Na pesquisa aplicada o objetivo é encontrar uma solução prática para um problema social imediato ou para as dificuldades de uma organização industrial/empresarial, ou seja, para uma situação concreta. Por sua vez, a pesquisa fundamental é dirigida no sentido de encontrar a informação que tem uma ampla base de aplicações e, portanto, contribui para o corpo organizado já existente do conhecimento científico. Neste último tipo de investigação o foco são as generalizações e a formulação de uma teoria.

Exemplos de pesquisa aplicada conforme Kothari (2004): aquela elaborada para identificar as tendências sociais, econômicas ou políticas que podem afetar determinada instituição. O autor dá como exemplos de pesquisa fundamental aquela que se debruça sobre algum fenômeno natural ou sobre a matemática pura. Ele explana ainda que estudos sobre o comportamento humano contínuo com o objetivo de definir generalizações são exemplos de pesquisa fundamental, mas a investigação destinada a encontrar uma solução para um problema social ou de negócios concreto é um exemplo de pesquisa aplicada. De acordo com esses conceitos, esta é uma pesquisa aplicada, pois procura encontrar uma solução para um problema social concreto.

Conforme Creswell (2003), a pesquisa qualitativa é fundamentalmente interpretativa. Isso significa que o pesquisador interpreta os dados. Para isso, ele inclui na pesquisa a descrição de um indivíduo ou sua configuração, analisa os dados por temas ou categorias e, finalmente, elabora uma interpretação ou tira conclusões sobre seu significado. O pesquisador qualitativo utiliza um raciocínio complexo multifacetado, iterativo e simultâneo.

Embora o raciocínio indutivo esteja presente em grande parte das pesquisas qualitativas (CRESWELL, 2003), tanto o processo indutivo como o dedutivo podem ser utilizados. O processo usado na elaboração da pesquisa também é iterativo, como um ciclo: coleta de dados e análise para reformular o problema e voltar à coleta de dados e à análise. Então, há atividades simultâneas de coleta, análise de dados e refinamento do problema da pesquisa. Desse modo, reitera-se que a pesquisa em tela é qualitativa, pois é essencialmente interpretativa.

Kauark, Manhães e Souza (2010) consideram que é descritiva a pesquisa na qual se tende a analisar os dados indutivamente. O processo e seu significado são os focos principais dessa abordagem. Ela visa a descrever as características de determinada

população ou fenômeno, ou o estabelecimento de relações entre variáveis. O fenômeno em estudo é um problema concreto da engenharia social.

Quanto ao horizonte temporal, a pesquisa é diacrônica. Segundo Marais e Mouton (1996), um estudo diacrônico envolve a investigação de unidades de análise sem considerar um período de tempo estendido. A pesquisa diacrônica pode ser aquela que trata o fenômeno em estudo sem um ponto específico no tempo. Essa categoria pode, por exemplo, eludir o estudo de cenários sem considerar o tempo – caso desta pesquisa.

Para Yin (2010), cada método de pesquisa tem suas vantagens e desvantagens, e com base no tipo de questão da pesquisa, no controle do pesquisador sobre os eventos comportamentais e no enfoque dos fenômenos contemporâneos sobre os históricos pode-se optar pelo método que se acredita ser o mais vantajoso.

O estudo de caso geralmente envolve as questões “como” e “por que”. Nele o investigador exerce pouco controle sobre os eventos, e o enfoque sobre o fenômeno contemporâneo está no contexto da vida real. Aqui a opção foram as técnicas da metodologia de pesquisa de estudo de caso para a coleta de dados. Foram utilizadas pastas eletrônicas sincronizáveis como instrumento de pesquisa. Foi nessa estrutura de pastas que o pesquisador manteve seu banco de dados. Essas pastas foram divididas em subpastas, nas quais foram guardados os achados da pesquisa, as conclusões do pesquisador e os trabalhos correlatos de outros pesquisadores. A ferramenta auxiliou a sincronização dos dados coletados em laboratórios diferentes, organizando os dados da pesquisa, o que aumentou o tempo para as análises, otimizando assim o tempo do pesquisador.

Outro instrumento utilizado foi um *software* criado para a coleta automatizada dos dados. O sistema fez pesquisas no Portal da Transparência de forma automática e coletou dados que correlacionam atores de redes sociais. Além disso, um questionário foi aplicado a alguns servidores públicos para gerar dados em diversas fontes de informação.

A validade *constructor*, que é uma garantia de credibilidade do estudo, segundo Yin (2010), é alcançada utilizando-se fontes de dados múltiplas. Os dados colhidos são de natureza específica: foram realizadas coletas de dados no Portal da Transparência. Yin defende que duas táticas podem ser usadas para superar as imperfeições de um estudo: o uso de protocolos e o desenvolvimento de um banco de dados do pesquisador. Todo o processo de pesquisa é baseado na busca de credibilidade da metodologia de pesquisa, portanto a formação de um banco de dados de pesquisa, a construção de questionários, entrevistas informais e a garantia da validade *constructor* foram criteriosamente

observadas.

Raupp e Beuren (2006) destacam que não se percebe na literatura pertinente uniformidade na abordagem das tipologias de delineamentos de pesquisa. Diversos autores têm organizado suas tipologias segundo a natureza da pesquisa, os objetivos, os procedimentos, os fins, os meios, as fontes de informação, etc. Selecionamos a tipologia quanto aos procedimentos de análise da pesquisa para descrever a metodologia utilizada – a análise de redes sociais (ARS ou SNA, da expressão em inglês *social network analysis*).

A ARS é uma abordagem oriunda da sociologia, da psicologia social e da antropologia (WASSERMAN; FAUST, 1994). A rede social é uma estrutura em forma de redes composta por nós geralmente representados por pontos, que nas ciências sociais são representados por sujeitos sociais (indivíduos, grupos, organizações, etc.), e por conexões entre eles, conectados por algum tipo de relação, normalmente representados por linhas que ligam os pontos, ou nós.

Silva et al. (2005) propõem a metodologia de ARS como uma ferramenta para a análise de produção científica, permitindo, por exemplo, a observação de alguns aspectos interdisciplinares da ciência da informação. Essa metodologia permite ainda que se testem algumas suposições sobre o comportamento social de um grupo em análise. Esses autores acreditam que a ARS pode ser utilizada para identificar e analisar fluxos de informações entre atores em organizações e empresas.

Nos últimos vinte anos vem crescendo o uso da ARS. Esse crescimento decorre do aumento da quantidade de dados disponíveis para esse tipo de análise, do desenvolvimento da computação e do processamento de dados – o aumento do poder computacional à disposição dos pesquisadores – e da ampliação dos assuntos de interesse, das áreas de conhecimento que utilizam a ARS e das inúmeras publicações sobre o tema (SILVA et al., 2005).

Yin (2010) ressalta que foram definidas variações para as ciências experimentais que estipulam que o pesquisador não pode manipular o comportamento, mas pode manipular a lógica do projeto experimental. Essas variações são chamadas de “quase experimentais” ou estudos “observacionais”. Para Yin, uma base de dados aumenta notavelmente a confiabilidade de todo o estudo de caso.

O núcleo da unidade de análise investigada na pesquisa foi o Portal da Transparência. Foram utilizados cenários extraídos da literatura para apresentar o risco e levantar hipóteses sobre ataques de engenharia social. Watson, Mason e Ackroyd (2014) defendem que cada cenário em segurança é formado pelo conjunto de vulnerabilidades e

objetivos de ataque. Além disso, todo cenário fundamentalmente deve possuir um alvo. Se não há alvo, não há ataque. Para os autores, os modelos de cenário podem ser utilizados em ataques iniciais ou ataques de iniciantes.

Foi construído um *software* para realizar diversas coletas automatizadas no Portal da Transparência. Os dados sobre compras de equipamentos de tecnologia da informação foram armazenados em uma base de dados relacional. Os dados coletados foram transformados em arquivos para que, com o *software* Pajek,[7] fosse possível a análise de redes sociais. A seção 2.4.1 apresenta mais detalhes sobre como foi realizada a coleta de dados por *software*.

Figura 3. Portal da Transparência

Fonte: http://www.portaltransparencia.gov.br/

O Portal da Transparência do governo federal (www.portaldatransparencia.gov.br) (**Figura *3***) é uma iniciativa da Controladoria-Geral da União (CGU) para garantir a publicidade e o controle social da aplicação dos recursos públicos. Ele divulga uma série de informações sobre servidores públicos, bem como informações sobre processos de aquisições de bens e serviços executados pelo governo.[8]

Em outra fase metodológica foram aplicados questionários, havendo a possibilidade de servidores públicos apresentarem vulnerabilidades. A intenção foi realizar um cruzamento entre os conhecimentos dos servidores sobre o tema, experiências desses servidores com fraudes e o interstício dos servidores para a entrada de problemas em engenharia social. A seção 2.4.2 apresentará mais detalhes sobre a pesquisa de opinião.

Os cenários presentes nas doutrinas e nas bibliografias serão discutidos no decorrer do trabalho e serão cruzados com casos concretos coletados na pesquisa de opinião com os servidores públicos. Os dados coletados no Portal da Transparência e os padrões

[7] O Pajek é um *software* esloveno utilizado para a análise de redes sociais. Para maiores informações consultar a seção 3.5.2.
[8] <http://transparencia.gov.br/sobre/OQueEncontra.asp>.

encontrados nas análises serão correlacionados com os casos e os cenários.

O propósito capital é analisar as redes sociais e estudar casos para encontrar possíveis alvos para ataques de engenharia social com o intuito de realizar a mediação – intermediação – da comunicação a fim de obter *insights* e possivelmente aplicar as recomendações para a segurança da informação. Portanto, a pesquisa em tela é aplicada, qualitativa, diacrônica e descritiva, tem como técnicas de coleta e análise de dados o estudo de caso e a análise de redes sociais. Trata-se de uma pesquisa quase experimental, pois, apesar de possuir testes e experimentos, o pesquisador não tem controle total sobre o ambiente.

Na **Figura *4*** está expresso o processo metodológico. Pode-se observar que ele se baseia na construção de pressupostos, utilizando para isso o arcabouço teórico e a articulação da fundamentação conceitual. A intenção é fundamentar os pressupostos de forma interdisciplinar com o uso da Ciência da Informação, da segurança da informação, da engenharia social, da confiança e da análise de redes sociais.

Dessa forma, a metodologia e a técnica de análise dos dados empregadas na pesquisa foram a ARS, pois além de verificar a manifestação das relações sociais estruturalmente, podendo a partir disso serem extraídas conclusões sobre o comportamento da rede social, ainda é possível avaliar o fluxo das informações que circulam na rede social em análise.

O estudo de caso foi utilizado para avaliar casos e consequentemente apresentar os riscos tanto nos cenários hipotéticos quanto nas entrevistas com membros de organizações públicas. O questionário utilizado encontra-se no Apêndice A – Questionário da pesquisa de opinião

Acredita-se que essa base conceitual possibilitará deduzir que a engenharia social implica confiança estabelecida e que a confiança é construída por meio da comunicação. Então, por meio da identificação de estruturas de comunicação – com o uso da análise de redes sociais e da identificação de possíveis vulnerabilidades –, da pesquisa de opinião, do estudo de caso utilizando cenários presentes nas doutrinas e nas bibliografias poderemos apresentar caminhos para a prevenção de ataques de engenharia social.

Mais especificamente demonstrou-se como computar informações de redes sociais com dados presentes no Portal da Transparência. Posteriormente, esses dados foram transformados em sociogramas no *software* Pajek para, enfim, serem selecionados alguns cenários para a discussão. Em todo esse processo foram considerados os questionários aplicados a servidores públicos.

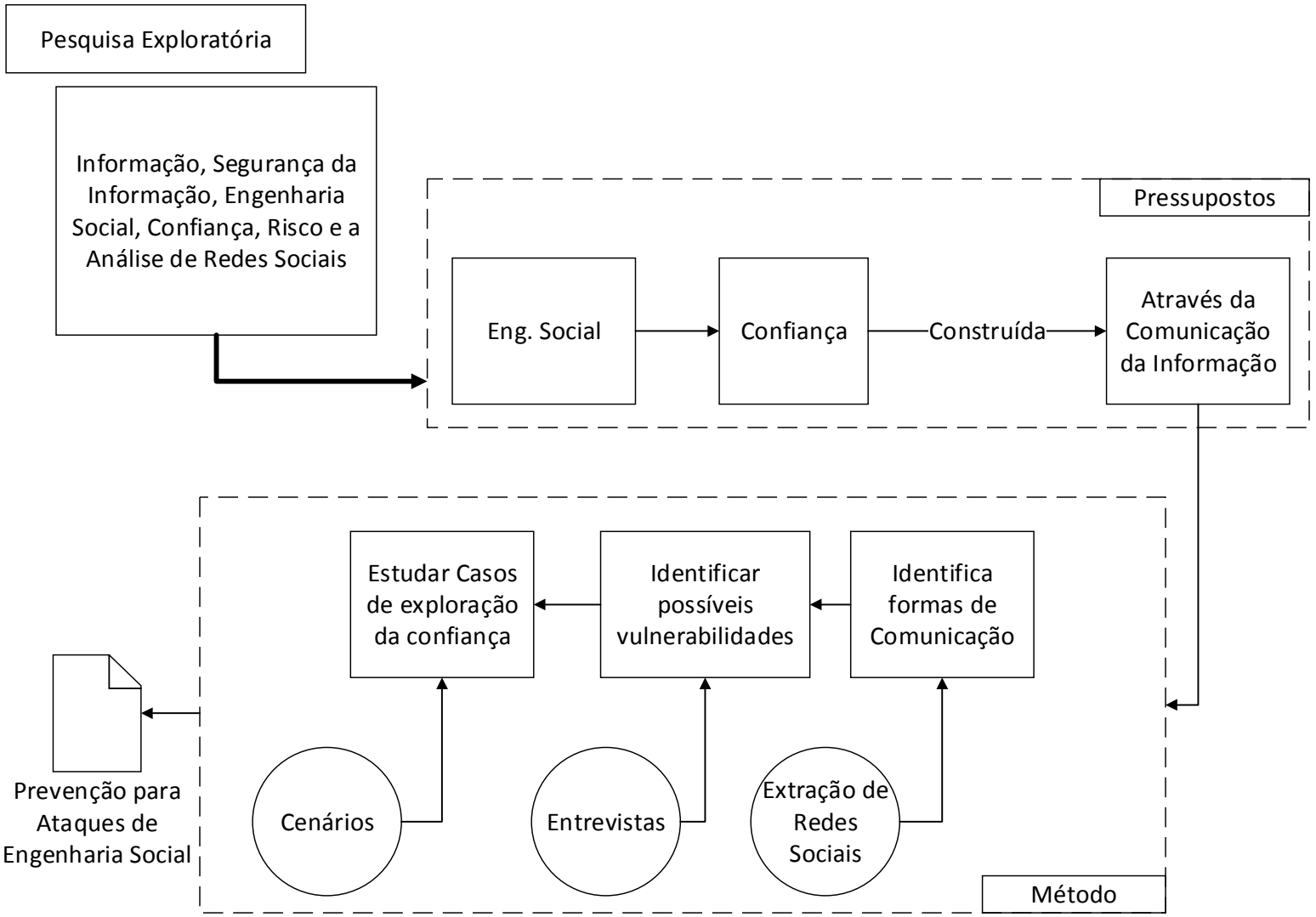


Figura 4. Processo metodológico

Fonte: elaboração do autor

2.4.1 Metodologia da coleta de dados

No mundo real, a complexidade geralmente torna difícil criar um experimento controlado. Além disso, a ética, os custos e a viabilidade impõem limites. Um aspecto vital da pesquisa científica é a capacidade de reunir dados objetivos e testar hipóteses (SHOSTACK; STEWART, 2008).

Shostack e Stewart (2008) afirmam que o campo da segurança da informação não está trabalhando tão objetivamente quanto deveria. Não estão sendo buscados dados objetivos de âmbito operacional. Tem-se trabalhado muito a segurança de detecção e resposta. Por meio da coleta de dados, da análise, da orientação, da decisão e da ação se pode aumentar o grau de confiança na segurança.

Russell (2013) demonstra como minerar dados em páginas web. O autor ensina que este é um problema de *information retrieval* (IR). Para essa mineração de dados, alguns métodos de processamento de linguagem natural podem ser utilizados, e geralmente esses métodos tratam os textos como “sacolas de palavras” que podem ser modeladas e manipuladas como vetores. Obviamente que se trata de algo sensível ao contexto e relacionado à semântica da linguagem humana.

É necessário definir três termos antes de prosseguir: *scraping, crawling* e *parsing*. Estas são expressões da língua inglesa que se preferiu não traduzir por uma questão de alinhamento com o jargão técnico e por não haver substitutas na língua portuguesa. Russell (2013) define *web scraping* como o processo de extração de texto de uma página web. Muitas vezes os códigos de programação e marcação tornam o trabalho de extração mais difícil. O *web scraping* faz esse trabalho minimizando as dificuldades, pois só retorna o texto que interessa. Por sua vez, o *crawling* consiste na extração de *hyperlinks* e na navegação entre eles, formando uma teia, por um sistema autônomo. Por fim, o *parsing* é o processo de análise de uma cadeia de caracteres conforme uma gramática específica.

Nas seções a seguir será mostrado como foram realizadas as coletas no Portal da Transparência.

2.4.1.1 Automação de coleta dos dados

A solução tecnológica escolhida é baseada em um robô que executa as funções de extração web, rastreador web e análise sintática (do inglês *web scraping, crawler* e *parsing*), construído em *software*. Nos Apêndices B ao D podem-se verificar alguns trechos desses

códigos em Python,[9] porém serão feitas algumas referências para situar a solução tecnológica no contexto da pesquisa. O tema não será discutido em detalhes por fugir ao escopo deste trabalho. O *software* executou uma varredura nas páginas do Portal da Transparência.

Inicialmente pensou-se em utilizar o arquivo que contém as compras do governo fornecido pelo próprio Portal da Transparência. Este oferece um arquivo consolidado com muitas informações sobre os gastos das unidades gestoras (UGs), que são entidades autônomas para empenho, alocação de recursos e pagamento no sistema financeiro da administração pública federal. Porém, o arquivo está bem consolidado, portanto não possui dados suficientes para nosso objetivo de pesquisa. Por isso optou-se por construir o robô em *software* para todas as coletas.

No Apêndice B está um exemplo de como foram coletados os órgãos superiores, os órgãos subordinados e as unidades gestoras. É importante informar que foi preciso uma carga de dados inicial para que o robô pudesse construir as consultas no Portal da Transparência.

Após descobrir que o Python seria a linguagem de programação utilizada, foi necessário entender como a ferramenta/linguagem Python poderia auxiliar na leitura e na transformação dos dados capturados do Portal da Transparência. A intenção era fornecer ao Pajek um arquivo com a rede social completa para análise. Os pacotes/bibliotecas para *scripts* Python Mechanize e BeautifulSoup auxiliaram, pois tanto simulam um navegador de internet como decodificam o HTML, respectivamente.

Inicialmente construiu-se um ambiente para simular a leitura de um *site* (PHP). Após os testes com os dados controlados em PHP passou-se à construção de um repositório de armazenamento com a intenção de realizar diversas consultas com mais facilidade. Para isso optou-se por utilizar a tecnologia de banco de dados relacional PostgreSQL. A próxima etapa foi observar como ocorrem alguns padrões de *software* no Portal da Transparência. Foram efetuadas consultas e observado o retorno com o Firebug, que auxilia na inspeção de códigos HTML.

Observou-se que no formulário de consultas avançadas era possível submeter pesquisas para automatizar o processo de filtro e coleta de informações, porém existiam

[9] O Python é uma linguagem interpretada de programação – aquela linguagem que não necessita de compilação – em *script* – arquivos de texto geralmente escritos em linguagem *english like.* Maiores informações em <http://www.python.org>.

algumas limitações, a saber:

1. encontraram-se problemas com a leitura de itens que utilizam tecnologia Ajax para atualizar dinamicamente o formulário;
2. após superar a barreira da leitura e da submissão com o Python em tecnologia Ajax, encontraram-se problemas com o bloqueio de acesso ao *site* via captcha.

Foi necessário utilizar um *proxy* na rede Onion para “enganar” o Portal da Transparência, simulando requisições de locais diferentes. A rede Onion, também conhecida pela sigla TOR, é uma rede de computadores distribuída com o intuito de prover meios de comunicação anônima na internet. A rede TOR é uma rede de túneis https sobrejacente à internet em que os roteadores da rede são computadores de usuários comuns. O objetivo principal do projeto é garantir o anonimato do usuário que está acessando a web.

Como a rede Onion troca os IPs de origem frequentemente, por meio de um controlador Python também é possível se trocar o IP quando quiser. O Portal da Transparência não solicitou a solução de enigmas captcha, e quando solicitado o sistema trocava o endereço de internet e executava novamente a consulta. Quando o Portal da Transparência retornar um captcha, a *thread* deve bloquear o uso do controlador do TOR e trocar o ID. As outras *threads* têm de ficar aguardando a liberação do controlador, verificar se o ID foi trocado e se não há captcha, prosseguindo com a consulta. O tratamento de exceção foi extensivo no *script*.

O programa central aciona várias *threads* que realizam consultas, buscando por palavras-chave nos retornos dessas consultas ao Portal da Transparência. No Apêndice C está um exemplo de como foram coletados os principais dados. Após encontrar alguma das palavras-chave a *thread* grava as informações da consulta no banco de dados, faz o *crawler* nos *links*, captura o favorecido, o valor da compra e as observações do documento de pagamento bancário – a ordem bancária (OB).

As principais necessidades e funcionalidades do sistema de coleta são: necessidade de carga de dados para poder preencher os formulários de pesquisa, a funcionalidade de consultar o Portal automaticamente, navegação entre os *links* dos hipertextos, montagem e exportação das redes sociais para o Pajek. As necessidades e as funcionalidades do experimento encontram-se na Tabela 1.

Tabela 1. Necessidades e funcionalidades

- **Necessidades e funcionalidades**

Necessidade 1		**Benefício**
Coletar dados de suporte a pesquisas no Portal da Transparência.		**crítico**
Identificação de funcionalidade	**Cenário previsto**	
F 1.0	São necessários dados de suporte a consulta. Por exemplo: unidade gestora ou dados do órgão.	
	Essa funcionalidade será executada uma vez para carga e posteriormente para atualização, caso necessário.	

Necessidade 2		**Benefício**
Pesquisar palavras-chave de forma que sejam encontrados *links* para navegação.		**crítico**
Identificação de funcionalidade	**Cenário previsto**	
F 2.0	Alarmar quando encontrar alguma das palavras-chave, presente em um dicionário, no conteúdo da página.	
	Encontrar *links* para navegação.	

Necessidade 3		**Benefício**
Navegar no *link* para encontrar detalhes do gasto.		**crítico**
Identificação de funcionalidade	**Cenário previsto**	
F 3.0	Navegar nos documentos de empenho ou gasto de outra natureza.	
	Armazenar informações dos tipos de equipamentos, valores, fabricantes, etc.	
	Será necessário um dicionário de fabricantes e equipamentos para a coleta.	

Necessidade 4		**Benefício**
Montar a rede social.		**crítico**
Identificação de funcionalidade	**Cenário previsto**	
F 4.0	Montar uma rede social baseada em parâmetros lidos de um arquivo.	
	Capturar informações de atores e relacionamentos segundo um critério parametrizado em um arquivo.	

Necessidade 5		**Benefício**
Exportar rede social para o Pajek.		**crítico**
Identificação de funcionalidade	**Cenário previsto**	
F 5.0	Exportar um arquivo de uma rede social para o formato “.net” do Pajek.	

Construiu-se uma base de dados PostgreSQL, simples, que possibilita e facilita a recuperação e a transformação dos dados para uma rede social. Rede de dois modos é o primeiro tipo de rede que o *software* gerará no formato .net – formato do *software* de análise de redes sociais Pajek, relacionando órgão e equipamentos sensíveis para as redes de computadores. Após essa etapa podem ser analisadas as redes com o Pajek. Foram feitos vários testes e uma análise de viabilidade do projeto.

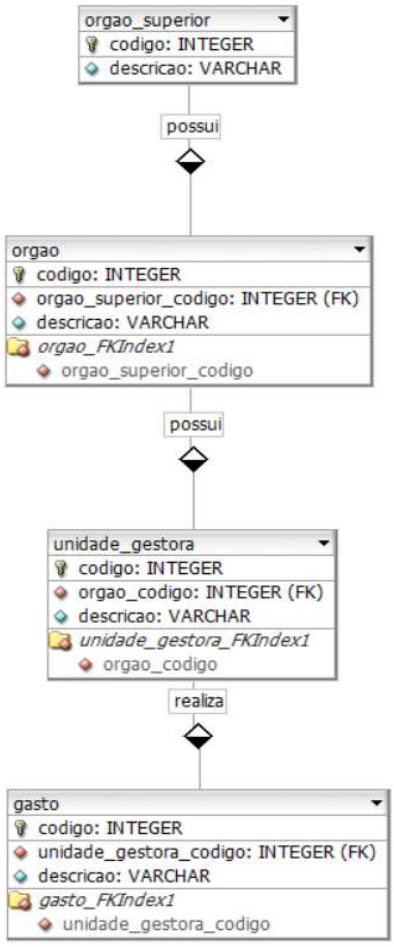


Figura 5. Modelo Entidade Relacionamento

Fonte: elaboração do autor

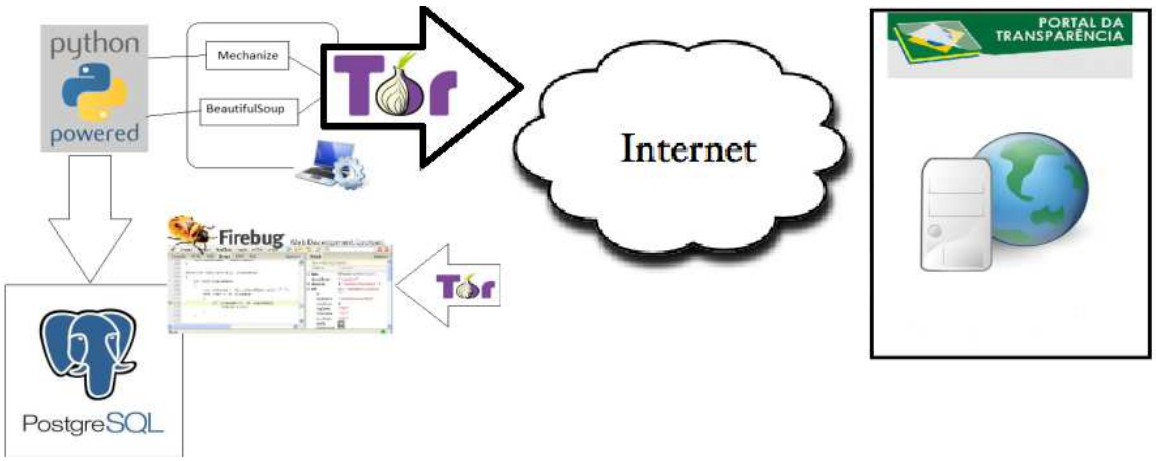


Figura 6. Modelo de solução tecnológica

Fonte: elaboração do autor

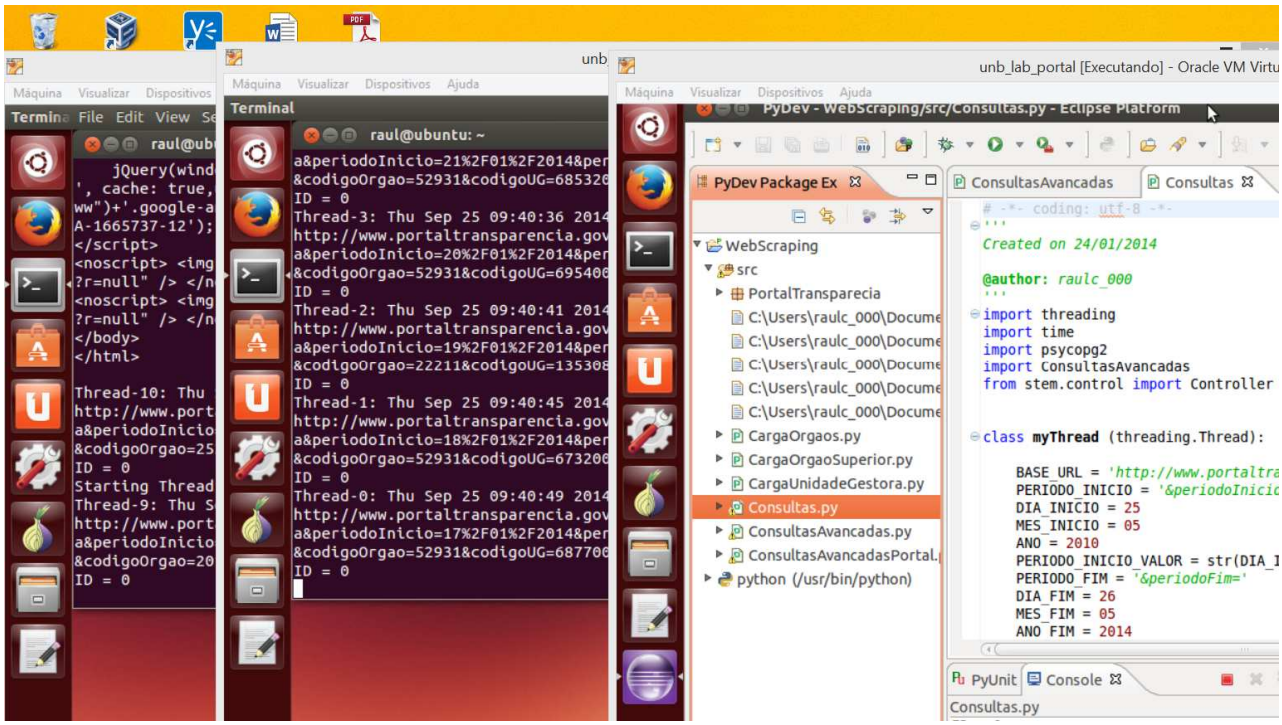


Figura 7. Captura de tela com máquinas virtuais executando *scripts* de coleta

Fonte: elaboração do autor

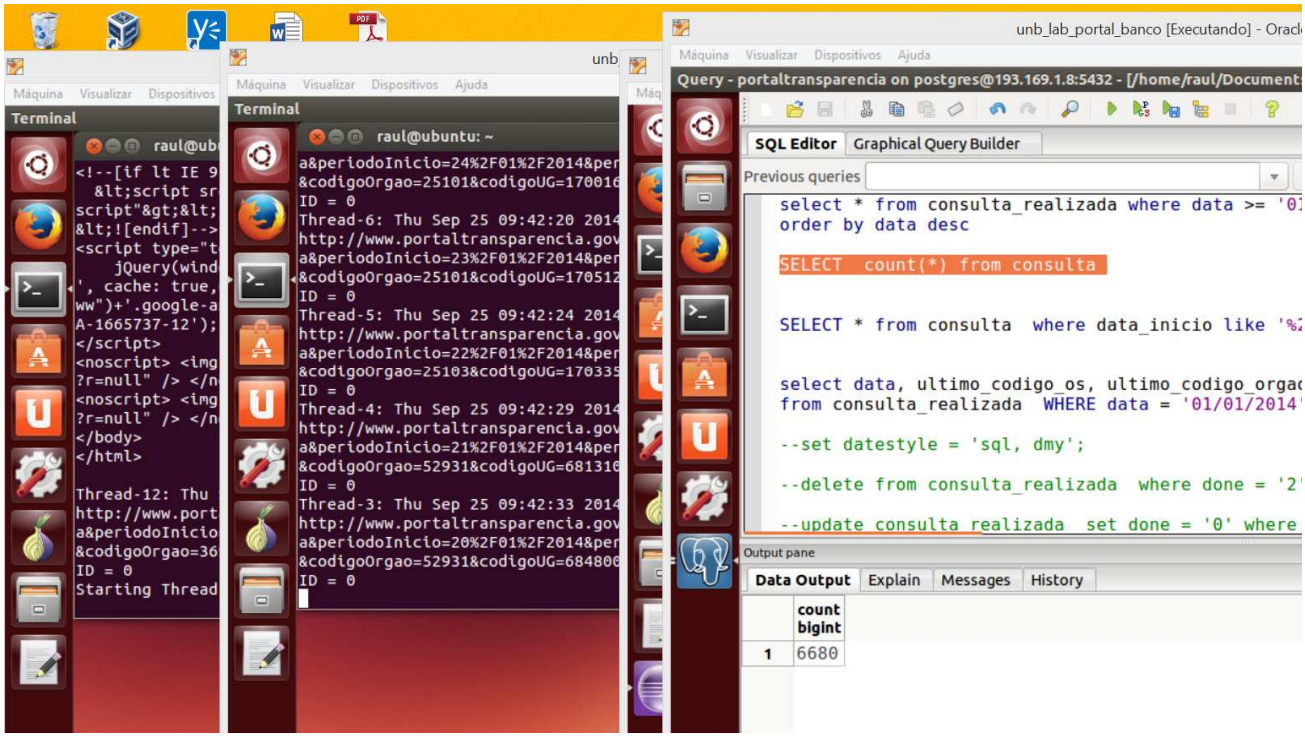


Figura 8. Captura de tela com máquinas virtuais executando *scripts* de coleta e banco de dados

Fonte: elaboração do autor

No Apêndice D está um exemplo de como o arquivo .net é criado. É importante observar que o arquivo segue o mesmo formato daquele apresentado na subseção 3.5.2. Além da criação da rede é criada uma partição que divide o contratante do contratado, em outras palavras: o favorecido e a unidade gestora.

Portanto, foi construído um *software* que realizou diversas coletas automatizadas no Portal da Transparência. Esses dados referentes a compras de equipamentos de tecnologia da informação foram armazenados em uma base de dados relacional (**Figura *5***). O *software* foi executado em diversas máquinas virtuais apresentadas nas **Figura *7*** e **Figura *8***.

2.4.2 Pesquisa de opinião com servidores públicos

A validade *construto* é uma validade qualitativa da pesquisa. Uma característica básica dos testes na validade de um construto é a convergência, ou seja, os resultados dos diferentes testes devem convergir. Diferentes testes podem significar diferentes fontes de informação. Portanto, para criar maior qualidade às afirmações apresentadas diante da questão de pesquisa foram consultados 45 servidores públicos lotados nas organizações constantes da Tabela 2.

Tabela 2. Organizações nas quais trabalham os servidores consultados

1.	Bacen – Banco Central do Brasil;
2.	CD – Câmara dos Deputados;
3.	CEF – Caixa Econômica Federal;
4.	CN – Congresso Nacional;

5.	Dataprev – Empresa de Tecnologia e Informações da Previdência Social;
6.	Dftrans – Secretaria de Transporte do Distrito Federal;
7.	GSIPR – Gabinete de Segurança Institucional da Presidência da República;
8.	Infraero – Empresa Brasileira de Infraestrutura Aeroportuária;
9.	PGR – Procuradoria-Geral da República;
10.	PMDF – Polícia Militar do Distrito Federal;
11.	PGDF – Procuradoria-Geral do Distrito Federal;
12.	Serpro – Serviço Federal de Processamento de Dados;
13.	SEDF – Secretaria de Educação do Distrito Federal;
14.	Não identificada.

O questionário encontra-se no Anexo 1. As perguntas foram construídas com o intuito de apresentar o contraste entre o conhecimento dos servidores sobre os temas aqui

estudados, sua disposição para ajudar qualquer um a finalizar seu trabalho cotidiano e a grandeza de trabalhos remotos realizados em sua organização, principalmente aqueles provenientes de autoridades, passíveis de exploração por um engenheiro social. A grande dúvida é se os cenários hipotéticos de engenharia social na administração pública se confirmam.

Os consultados relataram que tiveram conhecimento pessoal sobre golpes, fraudes, crimes via internet ou telefone, ou seja, eles sofreram ou conhecem alguém que sofreu com esse tipo de crime. Cinco consultados informaram que não tiveram contato pessoal com o problema.

Diante da complexidade das relações sociais, é preciso considerar a dificuldade em se prever toda e qualquer ação dos indivíduos. Portanto, faz-se necessário uma análise qualitativa do contexto para apreender a realidade de fato – casos concretos –, procurando uma anuência com as análises de dados automatizadas, possibilitando generalizações e a construção do entendimento sobre o tema seleção de alvos para engenharia social.

3 Fundamentos conceituais

3.1 A ciência da informação e a informação

Esta seção apresenta um posicionamento sobre o que vem a ser informação e apresenta basicamente a práxis dessa disciplina para se criar uma base e, então, estudar a segurança da informação.

O primeiro sinal de organização sistemática das informações no campo científico foi o trabalho bibliográfico de Johannes Trithemius *Liber de scriptoribus ecclesiasticis.* O controle e a divulgação de conhecimento acumulado foram iniciados com a imprensa e os primeiros livros. A obra *Traité de documentation*, de Paul Otlet (1934), foi um marco na sistematização da documentação científica (COSTA; LEITE; PIMENTA, 2013).

Pinheiro (2005) organiza o processo evolutivo da ciência da informação em décadas e de acordo com as publicações mais significativas, seguindo o mesmo modelo de Saracevic (1996). Costa, Leite e Pimenta (2013) consideram a década de 1950 a alvorada da ciência da informação como doutrina.

Em 1950, período de avanços pioneiros no processamento de dados com o auxílio de computadores, a chamada tecnologia da informação, na época conhecida apenas como informática, Calvin Mooers cunhou o termo *information retrieval*, que alcançou grande popularidade na área. Posteriormente, Farradane, em 1953, registrou a expressão *information scientist*, e em 1955 completou a operação criando o termo *information science* (COSTA; LEITE; PIMENTA, 2013).

Hoje praticamente tudo o que a sociedade faz utilizando a tecnologia da informação, em casa ou no trabalho, é registrado em computadores, o que favorece o controle sobre as atividades sociais. Segundo Saracevic (1995), a CI é inexoravelmente conectada à tecnologia da informação, talvez por isso ela deva ser utilizada como disciplina para o controle da confiança.

Na década de 1960 discutiu-se a natureza interdisciplinar da ciência da informação e foram construídas suas definições iniciais. Foi uma época de conflitos terminológicos com a informática nos mais diferentes países. A ciência da informação foi entendida como uma interface da documentação, da informática e da biblioteconomia, produzindo e propagando uma variedade de conceitos e definições. A recuperação da informação tornou-se uma atividade relativamente extensa, bem financiada e organizada, originando debates estimulados e acalorados acerca das melhores e mais adequadas soluções para o problema (PINHEIRO, 2005; SARACEVIC, 1996).

Nesse contexto destaca-se o artigo de Borko publicado em 1968 – “Ciência da informação: o que é isso?” –, porque contém as questões primordiais da CI como área científica, discutidas até hoje (PINHEIRO, 2005). Para o autor, a CI é uma ciência interdisciplinar proveniente e ligada à matemática, à lógica, à linguística, à psicologia, à tecnologia do computador, à pesquisa operacional, às artes gráficas, às comunicações, à biblioteconomia, à administração e a outros assuntos similares.

Borko (1968) define a CI como a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam o fluxo da informação e os meios que a processam para otimizar sua acessibilidade e sua usabilidade. Julga que o corpo de conhecimento dessa disciplina está relacionado à origem, à coleta, à organização, ao armazenamento, à pesquisa, à resposta, à interpretação, à transmissão e à utilização da informação. Para Borko (1968, p. 4), a CI pode ser aplicada nas seguintes categorias:

1. Necessidade e uso da informação:
   – estudos do comportamento dos usuários; estudos das citações; padrões de comunicação; estudos do uso da literatura.
2. Criação e cópia de documentos:
   – composição assistida por computador; microformulários; armazenamento e gravação; escrita e edição.
3. Análise da linguagem:
   – computação linguística; lexicografia; processamento de linguagem natural; psicolinguística; análise semântica.
4. Tradução:
   – tradução por máquina; tradução assistida.
5. Abstração, classificação, codificação e indexação:
   – sistema de classificação e indexação; análise de conteúdo; classificação assistida por computador; extração e indexação; estudo de vocabulários.
6. Desenho de sistemas:
   – centros de informação; recuperação da informação; mecanização das operações de bibliotecas; disseminação da informação sensitiva.
7. Análise e evolução:
   – estudos comparativos; qualidade de indexação; modelagem; métodos de teste e medição de *performance*; qualidade de traduções.
8. Reconhecimento de padrões:

– processamento de imagem; análise do discurso.

9. Sistema adaptativo:

– inteligência artificial; autômatos; solução de problemas; sistema de alto reconhecimento. (Tradução do autor.)

Na linha russa da CI, Mikhailov (1969 apud PINHEIRO, 2005) entende que a razão fundamental para a alvorada da informática não foi tanto o desenvolvimento dos produtos e das obras literárias, mas os aspectos intrínsecos ao estágio contemporâneo do desenvolvimento da ciência e da tecnologia. A informática surgiu para preencher um espaço que a ciência e a tecnologia necessitavam para avançar. Mikhailov é um autor russo que curiosamente utiliza a palavra *informatics* para denominar a ciência da informação.

Nas décadas de 1970 e 1980 emergiram trabalhos voltados à realização de experimentos matemáticos na formalização de fenômenos da ciência da informação. Houve um afunilamento das definições mais específicas dos fenômenos e dos processos que deveriam ser analisados pela CI. Foi o momento da busca por metodologias das ciências exatas, numa tentativa de elevar a CI ao *status* de ciência pura (PINHEIRO, 2005; SARACEVIC, 1996).

Consoante Goffman (1970 apud SARACEVIC, 1996, p. 46):

> O objetivo da disciplina CI deve ser o de estabelecer um enfoque científico homogêneo para estudo dos vários fenômenos que cercam a noção de informação, sejam eles encontrados nos processos biológicos, na existência humana ou nas máquinas [...] Consequentemente, o assunto deve estar ligado ao estabelecimento de um **conjunto de princípios fundamentais que direcionam o comportamento em todo o processo de comunicação e seus sistemas de informação associados** [...] (A tarefa da CI) é o estudo das propriedades dos processos de comunicação que devem ser traduzidos no desenho de um sistema de informação apropriado para uma dada situação física (grifo nosso).

De acordo com Saracevic (1975), a CI emergia como um tema de alta relevância, trazendo juntas a filosofia e a lógica para os assuntos das ciências humanas. O trabalho de Goffman “Ciência da informação: disciplina ou desaparecimento” (1970 apud PINHEIRO, 2005) é considerado inaugural nesse período, e seu título espelha a incerteza do momento. Pinheiro indica que provavelmente foi com essa preocupação que os profissionais da área introduziram a palavra ciência na denominação da CI, tal como fizeram os cientistas da computação.

Observa-se que as décadas de 1970 e 1980 constituem um período de grande produção no campo da CI. Em pouco mais de 15 anos surgiram teorias, disciplinas e

metodologias. Por exemplo, Harmon (1971 apud PINHEIRO, 2005) definiu as disciplinas que se inter-relacionam como disciplinas irmãs. Além disso, em seu trabalho expõe uma cronologia do surgimento das ciências do comportamento e da comunicação. A seguir apresenta-se a lista de disciplinas irmãs:

- 1933 – linguística, semântica;
- 1938 – Teoria do Valor;
- 1939 – Teoria da Decisão;
- 1944 – Teoria dos Jogos;
- 1945 – documentação;
- 1948 – Teoria da Informação, cibernética;
- 1950 – Teoria Geral dos sistemas;
- 1950 – formação das ciências da comunicação e do comportamento.

Para finalizar os setentistas e oitentistas, apresentam-se as ideias de Pooper (1972 apud BROOKES, 1980) e seus, bastante citados, três mundos. O autor, na obra *Objective knowledge*, apresenta os três mundos da informação.

1. O primeiro mundo é o mundo físico, aquele que existe de fato, o mundo das coisas naturais, o mundo assim como ele é, sem a intervenção da humanidade.
2. O segundo mundo é o mundo do pensamento humano, a subjetividade, o estado mental, a visão do mundo pelo homem.
3. O terceiro mundo é o mundo do conhecimento objetivo, os produtos do pensamento humanos gravados na arte, na língua, na ciência, nas coisas – tudo o que foi transformado pelo homem e armazenado no planeta Terra.

Esses mundos interagem por interseções, conforme defendeu Brookes (1980), e estão representados na imagem a seguir.

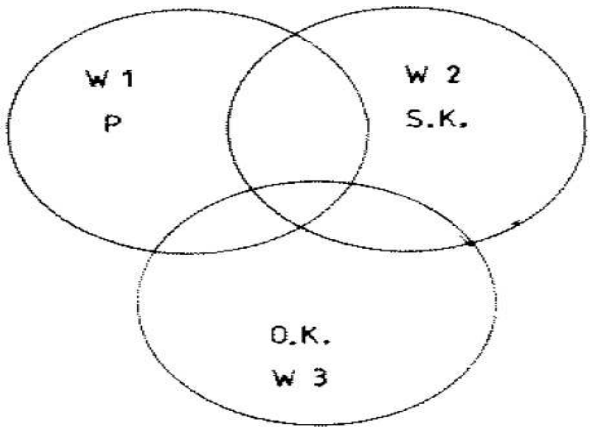


Figura 9. Os mundos de Popper
Fonte: BROOKES (1980)

Brookes (1980) ressalta que a teoria da ciência da informação quase não existe ainda. Para o autor, a ciência da informação opera ativamente em um oceano de aplicações práticas – que cada vez mais envolvem o computador – e busca as fundações teóricas para a informação na sua relação com o conhecimento.

A seguir destaca-se a equação fundamental de Brookes sobre o conhecimento, denominada por ele de pseudomatemática. Para o autor, o conhecimento é uma estrutura de conceitos ligados (*linked)* e seus relacionamentos, podendo este ser objetivo ou subjetivo, e cada pequena parte do conhecimento carrega a informação, gerando assim uma estrutura.

$$K[S]+\Delta I=K[S+\Delta S] \quad ,$$

onde **K[S]** é a estrutura de conceitos e delta **I** são as informações. O outro lado da igualdade representa as estruturas isomórficas, ou seja, aquelas iguais estruturalmente.

A relação entre conhecimento, informação e CI mereceu destaque na década de 1980 (PINHEIRO, 2005). O trabalho de Farradane (1980 apud PINHEIRO, 2005) esboça um conjugado do escopo da área e da natureza dos elementos por ela manipulados, isso auxiliou as conclusões do quão fortemente a área é ligada à cognição.

A década de 1990 foi o momento da consolidação da denominação e de alguns princípios, métodos e teorias, bem como do aprofundamento da discussão sobre a interdisciplinaridade da ciência da informação com outras áreas. Apesar da elaboração dos problemas ser mais concreta, nessa época ainda era preciso pensar a respeito do objeto

de pesquisa e dos fundamentos da área. Havia a preocupação de analisar conceitualmente a disciplina com a finalidade de exemplificar suas articulações centrais e seus conceitos básicos (PINHEIRO, 2005).

Nessa década, Capurro (1992, tradução do autor) analisa a Ciência da Informação como um ramo da retórica, que tem por base os três tipos de discurso de Aristóteles: o discurso deliberativo, o legal e o laudativo. “Inversamente ao pensamento da informação se tratar de um domínio descontextualizado ou elemento autônomo, as visões hermenêuticas e retóricas pressionam para a contextualidade (incluindo as dimensões éticas, culturais e políticas)”. O autor questiona a serventia da Ciência da Informação realizando um discurso retórico.

Pinheiro (2005) define que o trabalho de Capurro é muito importante por realizar uma reconciliação com a articulação entre CI e as tecnologias, geralmente julgadas com oposição aos aspectos socioculturais da Ciência da Informação.

Saracevic (1995) apresenta seu artigo sobre a interdisciplinaridade da Ciência da Informação, estudando a natureza e as tendências dessa ciência nas suas relações interdisciplinares. A evolução das relações interdisciplinares é verificada pelo autor no que concerne a quatro áreas: biblioteconomia, ciência da computação, ciência cognitiva, inteligência artificial e comunicação.

Bates (1999, p. 1045) defende que a Ciência da Informação tem na Teoria Geral do Sistema, na Teoria dos Jogos, na cibernética, na Teoria da Comunicação e na linguística sua força motriz:

> A Ciência da Informação não consiste apenas do explícito paradigma de estudo da seleção, da coleta, da organização, do acesso, e da recuperação de informação. Essa é a habitual descrição do campo. Tal como acontece com a maioria dos domínios intelectuais, o campo da Ciência da Informação tem muitas desarticulações, mas conta com importantes elementos “inferiores à linha de água” (tradução e grifo nosso).

Para Miranda (2002, p. 1), na acepção prática, como atividade profissional “a Ciência da Informação privilegia o registro do conhecimento conforme os métodos e as técnicas ao seu alcance, ou seja, fenomenaliza e problematiza a informação sobre a informação”, ou seja, o problema de estudo da Ciência da Informação é a construção de informações sobre a informação, estudar a informação em todos os seus aspectos.

Capurro e Hjørland (2003) corroboram outros autores da época apresentando que a Ciência da Informação é construída com base no conceito da biblioteconomia, da documentação e da computação. Eles destacam a Teoria da Informação como uma teoria

de grande influência em diversas áreas. Porém, houve problemas na aplicação dessa teoria porque o conteúdo da mensagem, segundo Capurro e Hjørland, não é considerado.

A Teoria da Informação considera a informação apenas nos aspectos de armazenamento e transmissão. Shannon (1948) informa que apesar de a mensagem ter significado, o aspecto da significância da mensagem é irrelevante para a engenharia no contexto de sua teoria. O problema estudado por Shannon é a reprodução da mensagem de um ponto a outro. Os sistemas, para o autor, têm de ser desenhados para operar cada possibilidade da mensagem transmitida, independentemente de seu significado.

Capurro e Hjørland (2003) apresentam os paradigmas físico, cognitivo e social da seguinte forma:

- o paradigma físico é fortemente influenciado pelas teorias de Claude Shannon e Waren Weaver;
- o paradigma cognitivo leva à ontologia e à epistemologia de Karl Pooper e Brookes;
- o paradigma social está associado à hermenêutica; analisa os indivíduos em situações concretas, nas organizações, em seus diferentes papéis.

Para estudar a Ciência da Informação é importante conceituar ciência e informação. Ciência é a produção ou a prática para a construção do conhecimento ou o conhecimento em si. Shostack e Stewart (2008) afirmam que se uma situação não pode ser testada, é uma crença – e não ciência –, e a maneira ideal de se testar uma hipótese é fazendo experimentos. Nascimento (2008) doutrina que para entender o que é a Ciência da Informação seria necessário observar com rigor e descrever com exatidão o que se denomina informação. Nascimento (2008, p. 74) afirma:

> Todas as disciplinas acadêmicas têm foco em diferentes universos dos fenômenos. As ciências naturais estudam o mundo natural; as ciências sociais estudam o mundo social produzido por humanos e as artes e as humanidades estudam o conteúdo e o contexto das atividades criativas dos seres humanos, desde a filosofia até a literatura e as artes. A Ciência da Informação tem um universo distinto que estuda o mundo das informações registradas produzidas pelos agentes humanos sem, no entanto, focalizar seu conteúdo.

Zins (2007) demonstra que não há aparentemente um conceito uniforme sobre a Ciência da Informação. Por intermédio de uma metodologia Delphi consulta diversos especialistas que divergem em suas definições, porém convergem quando afirmam que a CI se preocupa em trabalhar alguns conceitos, como dados, informações, conhecimento e

mensagem (**Figura *10***).

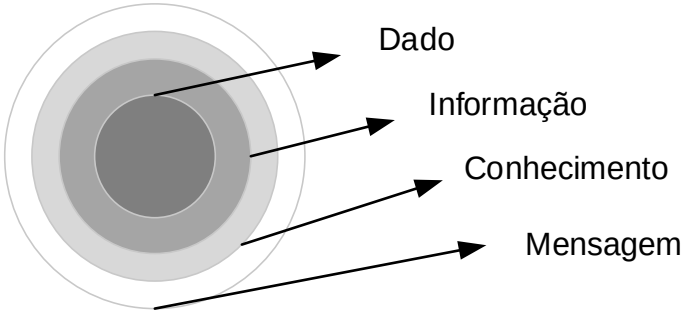


Figura 10. Relação entre dado, informação, conhecimento e mensagem

Fonte: ZINS (2007; tradução do autor)

Silva et al. (2005), sob a perspectiva da Ciência da Informação (CI), afirmam que as ligações estudadas por meio da análise de redes sociais nas organizações são capazes de identificar e analisar os fluxos de informação. Para os autores, pode-se utilizar a análise de redes sociais para avaliar as comunicações entre atores sociais de modo que se obtenham informações vantajosas. Silva e Ferreira (2007) explicam que os estudos baseados na ARS nas empresas foram, em geral, realizados com a intenção de estudar os fluxos de informações e seus efeitos sobre os atores sociais.

Para finalizar a fundamentação conceitual sobre a CI apresenta-se a arquitetura da informação (AI), que surge para o desenvolvimento de uma nova disciplina. Uma ciência, uma prática, uma arte de transformar o “mundo” imaterial por meio da manipulação dos objetos no “mundo” material. Macedo (2005, p. 132) define

> Arquitetura da informação como uma metodologia de desenho que se aplica a qualquer ambiente informacional, sendo este compreendido como um espaço localizado em um contexto; constituído por conteúdos – em fluxo; que serve a uma comunidade de usuários. Entende-se como sua finalidade maior viabilizar o fluxo efetivo de informações por meio do desenho de ambientes informacionais.

Siqueira (2012, p. 220) ensina:

> Práxis é o conjunto de atividades e práticas, decorrentes do Conhecimento, realizadas pelo sujeito no labor, no trabalho e na ação para adequar a realidade ao seu entendimento e propósitos. É o fundamento da tecnologia. É através da práxis que o arquiteto de informação modifica os espaços sob os quais atua através de novas configurações da informação. Ele o faz criando ou modificando artefatos. […] o resultado da práxis da arquitetura da informação é uma nova configuração dos entes e relações no mundo, considerado pelo sujeito como alvo de sua intervenção. Esta intervenção se dá, no âmbito da disciplina de arquitetura da informação, pelo

> uso das quatro categorias fundamentais definidas na Teoria da Arquitetura da Informação: manifestação, forma, contexto e significado.

A arquitetura da informação organizacional é o *framework* que define o núcleo, os princípios, o modelo arquitetural, os padrões e os processos que formam a base para produzir informação confiável e segura em uma organização (GODINEZ et al., 2010).

Para Rosenfeld e Morville (2002), os usuários, o contexto e o conteúdo do espaço informacional são a base para um modelo prático e efetivo do desenho de uma arquitetura da informação, em suma:

- os usuários são aqueles que utilizam a informação;
- o contexto é o ambiente no qual a informação e os usuários estão inseridos, é a situação cultural e econômica, o contexto da missão organizacional;
- o conteúdo é o dado, os metadados, ou seja, é todo o objeto que se necessita para construir a informação.

Devido à amplitude desses três elementos – usuário, contexto e conteúdo –, a análise dos problemas na AI é considerada complexa e eleva cada caso a um caso particular. Todo o processo de classificação, modelagem, desenho, análise dos dados, informações e conhecimentos de uma organização desde o surgimento descentralizado até o controle central pela alta administração pode ser auxiliado pela AI (ROSENFELD; MORVILLE, 2002).

Figura 11. Elementos da arquitetura da informação (AI)

Fonte: ROSENFELD; MORVILLE (2002)

Nascimento (2008, p. 83) defende que:

> A arquitetura da informação, na visão tradicional, é considerada como a área da Ciência da Informação envolvida com os meios de processamento para otimizar a acessibilidade e a usabilidade da informação e seus fluxos. Seu objetivo estaria

> voltado para a organização e a recuperação da informação para tornar o fluxo mais efetivo. Nesse enfoque conta com o apoio de tecnologias da informação.

Definir a arquitetura da informação é um desafio intrínseco à linguagem e à representação das coisas. Ela pode ser interpretada como a combinação de organização, rotulagem e construção de esquemas de navegação para sistemas de informação. Também é conhecida como o desenho estrutural da informação no espaço para facilitar a resolução de tarefas e promover o acesso ao conteúdo. É uma disciplina emergente, focada na busca por princípios para o desenho, a modelagem no espaço informacional. Além disso, é conhecida como a arte e a ciência de estruturar e classificar a informação para auxiliar as pessoas a resgatar e a administrar suas informações (ROSENFELD; MORVILLE, 2002).

Encontrar esse desenho, essa estrutura e esse modelo de arquitetura da informação é um problema complexo, principalmente porque possuímos muitas informações e existe grande influência das relações sociais no espaço informacional. Existem cada vez mais informações circulando no espaço informacional. Rosenfeld e Morville (2002) esclarecem que classificar, mapear e estruturar as informações organizacionais pode ser comparado ao problema da previsão do tempo devido a sua complexidade.

Então, a arquitetura da informação, além de outras associações, está envolvida com a estruturação e o entendimento do fluxo de informação em um espaço informacional. Podemos entender que a construção de sociogramas na ARS seria uma forma de arquitetura da informação, tendo os analistas de segurança como usuários, os dados coletados para análise como conteúdo e o contexto da segurança da informação na entidade em análise como os elementos para o processo arquitetural.

Após todas essas explicações entende-se sucintamente o que é Ciência da Informação – que basicamente trata da recuperação, da coleta, da seleção da organização, da análise e do armazenamento da informação, porém não é só isso, e sim tudo circunscrito a isso. Mas, afinal, o que é informação?

Definir informação é obviamente o desafio central inerente à Ciência da Informação. A seguir algumas referências serão exibidas para se criar um posicionamento sobre o termo. Adianta-se que não houve uma conclusão ou um achado de pesquisa que possibilitasse uma definição absoluta sobre o que vem a ser informação. Mas é preciso construir um posicionamento para posterior definição do que vem a ser a segurança da informação.

Sloman (2007) opina que informação é um termo muito abstrato, assim como o termo energia, existindo diversas e diferentes formas e expressões para defini-la. Lombardi

(2004), ao tentar elucidar o que vem a ser informação, afirma que é necessário criar uma terminologia específica, mas não a cria, acredita que por não haver um consenso sobre o termo existe certa confusão conceitual quando a palavra informação é usada. Para ele, “a explosão das telecomunicações e da ciência da computação dotou o termo informação de prestígio científico, e por isso parece que se tornaram desnecessários maiores esclarecimentos sobre ele na sociedade (tradução do autor, p. 105).” Lombardi apresenta a conceituação de informação com enfoque físico, tomando por base as teorias de Shannon e o paradigma sintático que utiliza conceitos de probabilidade para conceituar informação.

O que se pôde apreender das explicações de Lombardi (2004) é que no paradigma físico a informação está ligada diretamente à comunicação. Para ele, de fato, a observação é uma forma de percepção da informação, em que o processo de transmissão da informação existe, estando presentes todos os elementos do enfoque físico. Mais adiante esse enfoque será mais bem estudado. O autor refere que o paradigma sintático é uma nova visão. Nesse paradigma, muitas de suas contribuições sequer citam os termos emissor, receptor e mensagem, que são a base do enfoque físico. Essencialmente essa conceituação sintática define informação como variações probabilísticas de organização dos signos.

É interessante verificar que a organização de padrões, abordagem sintática, também é referenciada por Bates em outro contexto, mas ainda sobre o propósito de um estudo terminológico a respeito da informação. Observe-se o que diz Bates (2005):

> Quando a informação é aqui definida como o padrão de organização da matéria e da energia, existem padrões de organização no universo existindo ou não vida em qualquer lugar nele. Há uma forma e uma estrutura em uma rocha aqui e uma forma diferente e uma estrutura em uma outra rocha ali, querendo ou não todos os animais veem rochas. Ao mesmo tempo, na medida em que a vida passa, é útil para os seres viventes perceber e interagir com seus ambientes. Como cada ser vivo experimenta seu ambiente tem enormes variações e algumas semelhanças. Meu padrão de organização não é o seu padrão de organização, mas, ao mesmo tempo, ambos vivemos no mesmo mundo e podemos estar respondendo a praticamente as mesmas coisas. O ponto aqui é que há muitos padrões de organização da matéria e da energia; algo acontecendo no universo independentemente dos seres que experimentam, assim como existem todos os vários padrões de percepção e experiências de organização que os animais desenvolveram a partir de suas interações com o mundo. Todos esses padrões de organização podem ser encarados do ponto de vista de um observador como informação (tradução e grifo do autor).

Capurro e Hjørland (2003) doutrinam que a informação é *prima facie* de algo que flui

entre um emissor e um receptor em uma comunicação. Segundo os autores, a informação é um conceito altamente ligado à manifestação do conhecimento, ou seja, a informação é relacionada a formas e estruturas de modelos mentais ou ligada à transmissão do conhecimento. Ainda conforme os autores, a informação não necessita de interpretação para existir, ela é sensível ao contexto e possui um significado, mas ela existe independentemente de um significado.

Como se estudou anteriormente, Pooper (1972, apud Brookes 1980) tratou da percepção da informação em seus três “mundos”: o mundo físico, o mundo do pensamento e o mundo do conhecimento objetivo. O que pôde ser concluído é: a informação existe sem haver a necessidade de sua percepção, porém a percepção só existe se há informação.

Zins (2007b), quando estudou o conceito de Ciência da Informação, concluiu que nesse campo algo é certo: a informação, o dado e o conhecimento são aspectos convergentes na CI. Quando se estuda CI, estuda-se dado, informação e conhecimento. No seu mapa de conceitos da Ciência da Informação a dialética sobre os conceitos de dados *versus* informações *versus* conhecimentos *versus* mensagens é o fenômeno explorado pela Ciência da Informação.

Veja-se, nessa linha, o que o dicionário *Merriam-Webster’s* apresenta sobre dado, informação e conhecimento. Após, poderá ser observado que os termos dado, informação e conhecimento estão intrinsecamente ligados quando utilizados para suas definições:

- dado é a informação factual (como medidas ou estatísticas) usada como base para o raciocínio, a discussão ou o cálculo;
- informação é a comunicação ou a recepção do conhecimento ou da inteligência; informação é o conhecimento obtido por meio de investigação, estudo ou instrução; informação é um ou mais dados;
- conhecimento é o entendimento obtido por meio da experiência; conhecimento é um conjunto de informações; conhecimento é a percepção clara da verdade.

A conclusão extraída desta seção é que a Ciência da Informação é interdisciplinar, focada no entendimento do que vem a ser informação e de todo o universo no qual a informação se insere. Mas o fato de existir informação não significa que haja Ciência da Informação. Porém, se existe Ciência da Informação há informação. Apesar de o objeto de estudo desta ciência estar em constante evolução, principalmente por este ainda não ter

uma definição objetiva, a CI tem um objeto de estudo, que é a informação, e se vale tanto de aspectos da ciência pura como da ciência aplicada para se desenvolver, apesar de atualmente ser conhecida por identificar-se melhor com a última.

3.2 Comunicação e mediação da informação

A comunicação é fundamental para a sociedade e é objeto de estudo de diversas disciplinas: engenharia, ciências naturais, ciências humanas, etc. Há quem defenda que o que diferencia a humanidade das outras comunidades de espécies de seres vivos é a efetividade da comunicação. Para este trabalho, o interesse pela comunicação é no sentido de ela ser um dos meios pelo qual a cooperação entre indivíduos acontece, aflorando aí o sentimento de confiança em sua plenitude, como se verá adiante. Aqui consideramos todos os tipos de comunicação entre humanos, seja verbal, seja corporal, escrita, em vídeo, imagem, por meio de objetos, etc.

Não há registros de como surgiu a comunicação humana. Sustenta-se que a comunicação falada se tenha iniciado com grunhidos e gritos (BORDENAVE, 1997). Em sua fantástica evolução, de grunhidos e gritos nossa comunicação chegou até o espaço sideral.

Em um exemplo menos cósmico, pode-se recordar da importância da gramática, que representa um avanço na comunicação. Nela há regras que determinam como os signos se combinam. A comunicação seria praticamente inviável se não houvesse as regras para organizar a utilização dos signos (BORDENAVE, 1997). Por exemplo, podemos diferenciar “Bob está comunicando signos com Alice” da frase “Alice está comunicando signos com Bob”. Mesmos signos, mas frases e semânticas diferentes devido à ordem dos signos e às regras gramaticais.

Berlo (2003) informa que o norte-americano passa 70% do seu tempo ativo se comunicando verbalmente: ouvindo, falando, lendo e escrevendo. Este pesquisador alerta para outras formas de comunicação: gestos, expressões e meios não verbais. Para Berlo, a comunicação é composta de emissor, receptor, canal e mensagem. Ele destaca que nem sempre quem recebe a mensagem é o receptor para o qual ela foi pensada e construída, ou seja, quando a mensagem é lançada no canal, outro receptor pode copiá-la.

Aristóteles definiu o estudo da retórica como a procura de “todos os meios de persuasão”. Nas comunicações de massa a retórica é fundamental, as mensagens, geralmente chegam a mais de um receptor. Berlo (2003) considera que a finalidade da

comunicação é a retórica, ou seja, a persuasão.[10] O interessante do pensamento de Berlo é seu entendimento de que toda mensagem tem uma audiência a ser influenciada. Isso pode fazer alguém pensar na engenharia social, que será estudada adiante.

Bordenave (1997) leciona que a comunicação, além de vencer o tempo e a distância, é impossível de não ocorrer. Por sua vez, Costa e Leite (2013) expõem que o fenômeno da comunicação é complexo e praticamente imperfeito e pouco efetivo – as pessoas comunicam-se efetivamente em raras ocasiões ou comunicam-se muito pouco, independentemente da quantidade de mensagens trocadas. A comunicação é um fenômeno grandioso que ocorre a todo o momento, seja por gestos, seja por olhares, sinais ou expressões faciais. Mensagens estão sendo transmitidas, muitas vezes involuntariamente, e recebidas a todo o momento pelas pessoas.

Inicialmente o estudo da comunicação foi estimulado pela necessidade do entendimento da influência do discurso político e posteriormente pela influência do cinema e do rádio. O estudo da comunicação entre indivíduos, que é uma das principais atividades-fim da comunicação e da mediação da informação na CI, é centrado no estudo de modelos de comunicação. Os modelos de comunicação da informação são divididos em lineares, circulares e transacionais (COSTA; LEITE, 2013).

Esses modelos não são completos e não representam a totalidade da realidade, mas são muito importantes para ajudar nas reflexões sobre problemas e fenômenos complexos (KROGERUS; TSCHÄPPELER, 2011). Para Mcquail e Windahl (1993), os primeiros modelos de comunicação são os lineares. Após a Segunda Guerra Mundial a comunicação começou a ser vista com um foco científico. Estudos empíricos foram largamente aplicados na comunicação. Foi nessa época que ocorreram as primeiras discussões a respeito da ciência da comunicação, terreno fértil para a criação de modelos de comunicação. Os estudos de Claude Shannon (Figura 14) foram bastante influentes nesse período.

O americano e cientista político Harold D. Lasswell apresentou um artigo em 1948 contendo a famosa frase no campo da pesquisa em comunicação: “O meio conveniente de descrever um ato de comunicação é respondendo às seguintes questões: Quem diz o quê? em qual canal? Para quem? Com qual efeito?”. Essas questões passaram a ser conhecidas como a fórmula de Lasswell (LASSWELL, 1948; MCQUAIL; WINDAHL, 1993), estruturada na Figura 12.

[10] A persuasão seria a tendência de se levar o outro a adotar o mesmo ponto de vista. A persuasão tem o propósito de induzir alguém a aceitar uma ideia, uma atitude ou realizar uma ação.

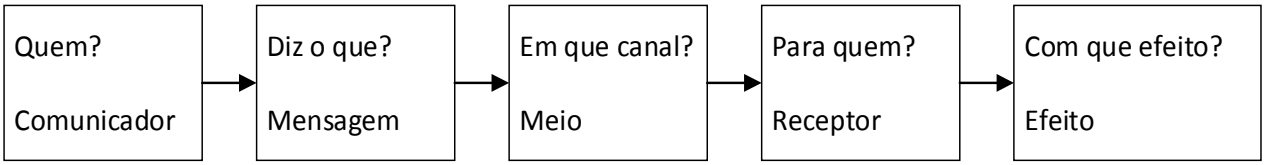


Figura 12. Fórmula de Lasswell em modo gráfico

Fonte: MCQUAIL; WINDAHL (1993; tradução do autor)

Verificou-se em Mcquail e Windahl (1993) que Braddock, em 1948, propôs uma extensão do modelo de Lasswell. Ele afirmou que deveriam existir mais algumas considerações além das cinco apresentadas. Na versão de Braddock foram incluídas mais duas facetas: a circunstância de envio da mensagem e o propósito da comunicação. Tanto Lasswell quanto Braddock não incluíram em seus modelos o elemento *feedback*. Na Figura 13 encontra-se o modelo de Braddock.

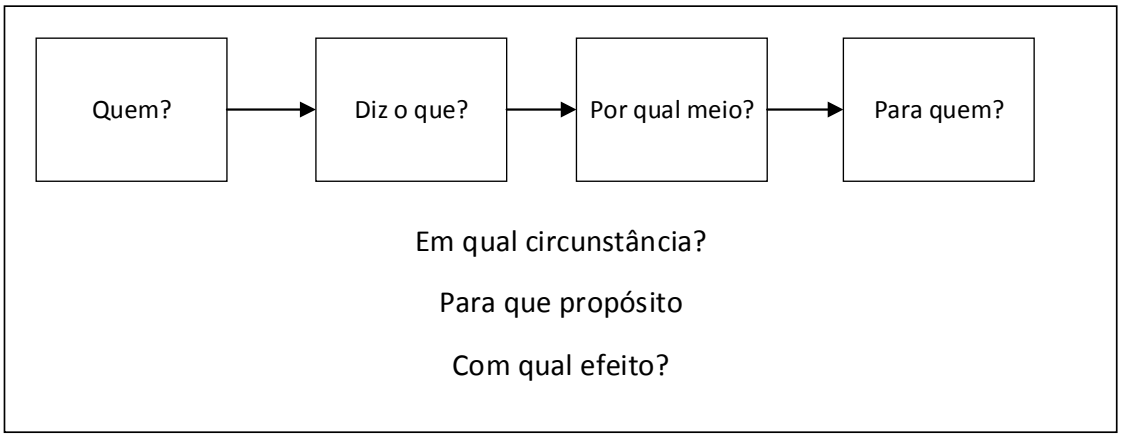


Figura 13. Extensão da fórmula de Lasswell proposta por Braddock

Fonte: MCQUAIL; WINDAHL (1993; tradução do autor)

O modelo de Shannon (1948) pela abordagem técnico-matemática é considerado o mais influente entre os modelos lineares. Shannon acrescenta o elemento ruído, comprovando que a mensagem, apesar de ter significância semelhante, não é idêntica nos dois lados – fonte e destino.

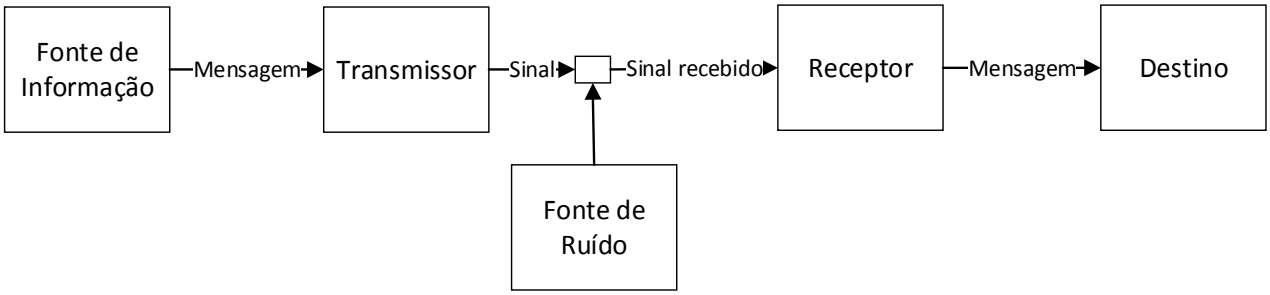


Figura 14. Modelo de Shannon

Fonte: MCQUAIL; WINDAHL (1993; tradução do autor)

Dance, em 1967, contesta os modelos lineares e os modelos circulares por não representarem retroalimentação e não traduzirem o incremento dos processos de comunicação, respectivamente. Na tentativa de solucionar os problemas dos modelos existentes na época, Dance apresenta seu modelo hélice para os processos de comunicação. A impressão de crescimento que a hélice apresenta revela a natureza incremental de seu modelo. Além disso, o modelo helicoidal é influenciado pela curva anterior, seguindo o pensamento de que os processos de comunicação têm suas interações influenciadas pelos eventos comunicativos ocorridos (MCQUAIL; WINDAHL, 1993).

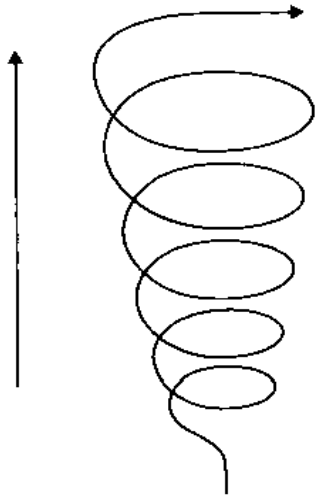


Figura 15. Modelo helicoidal de Dance

Fonte: MCQUAIL; WINDAHL (1993)

De Fleur desenvolveu, em 1970, um modelo inspirado no trabalho de Shannon e Weaver, introduzindo o mecanismo de *feedback*. Ele defendeu que no processo de comunicação o significado é transformado em mensagem e descreveu como a mensagem se transforma em informação. Por sua vez, a informação trafega por um canal, no qual o receptor entende a mensagem por meio da interpretação da informação. De Fleur afirma

que a mensagem tem correspondência de significado tanto no emissor quanto no receptor, porém a correspondência não é perfeita (MCQUAIL; WINDAHL, 1993). Na Figura 16 encontra-se o modelo de De Fleur.

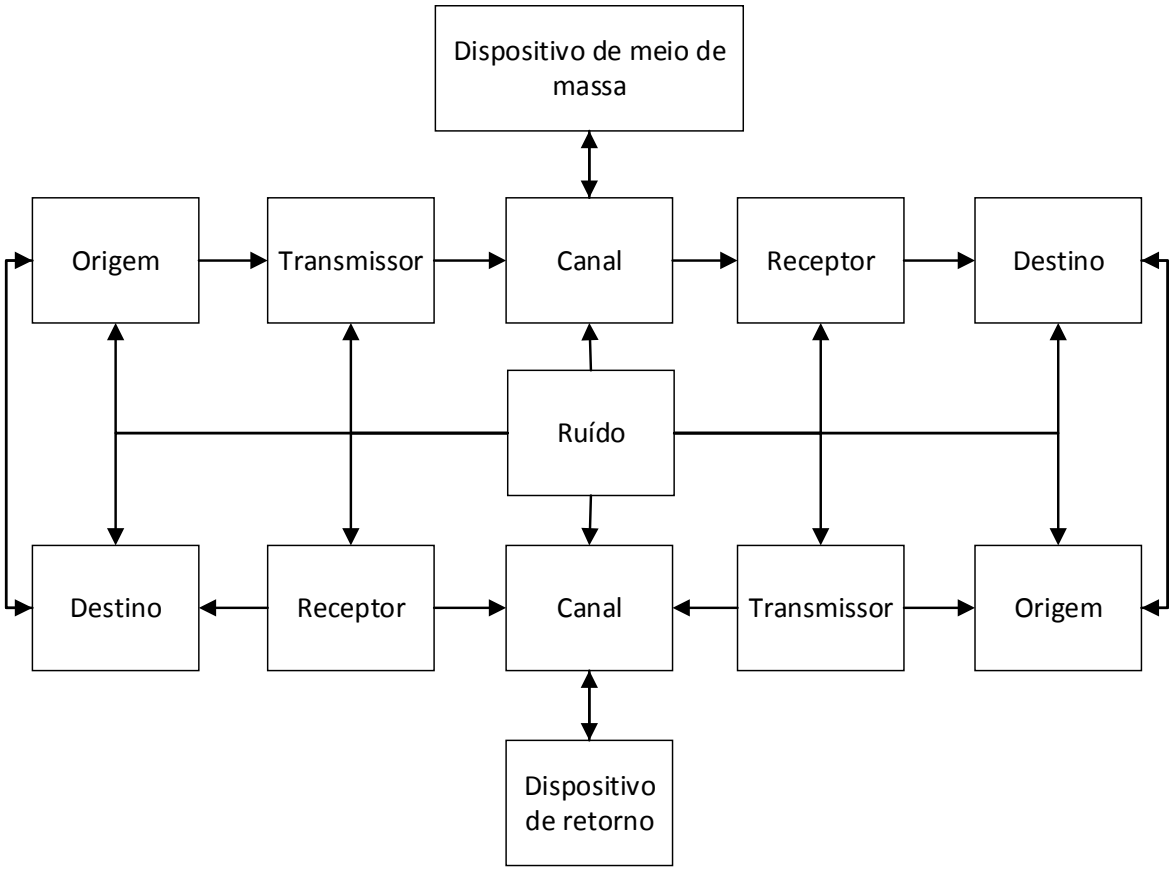


Figura 16. Modelo de De Fleur, inspirado em Shannon e Weaver, adicionando *feedback*
Fonte: MCQUAIL; WINDAHL (1993; tradução do autor)

Tubbs (2003) apresenta uma evolução nos modelos de comunicação. Segundo o autor, seria mais interessante observar seu modelo em animação. O modelo representa a comunicação básica, entre duas pessoas, chamadas por ele de comunicador 1 e comunicador 2. Ambos os comunicadores são fonte de comunicação, ou seja, originam e recebem mensagens simultaneamente. Tubbs traz em sua explicação o fator humano na comunicação, apresentando que ambos os comunicadores são influenciados pela mensagem. O modelo transacional é focado na simultaneidade da comunicação, tanto dos papéis dos comunicadores como na influência que o contexto tem sobre a comunicação.

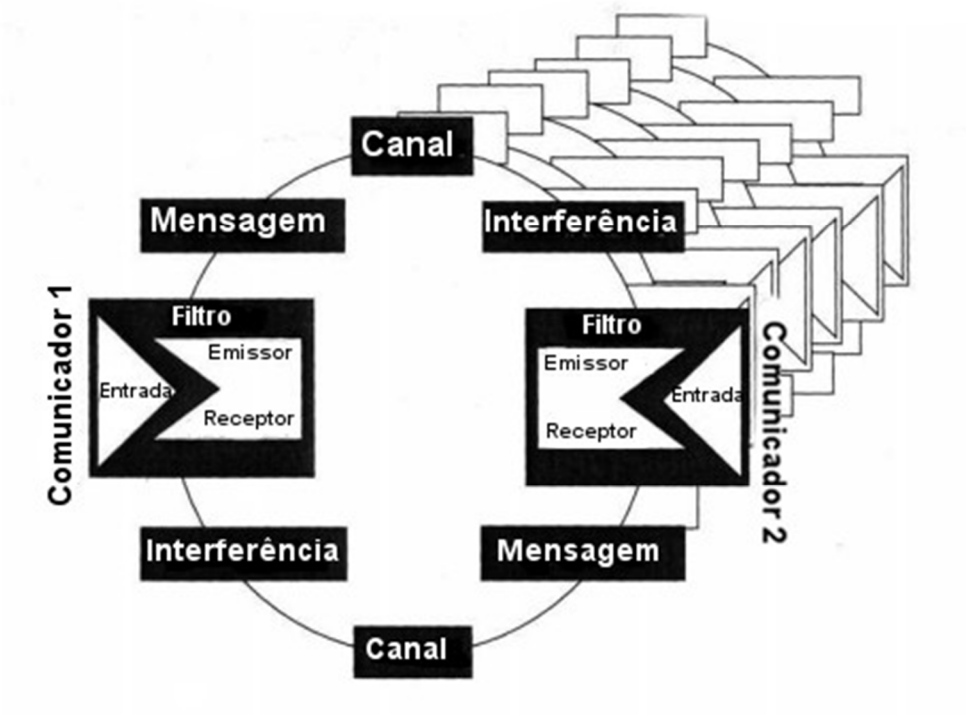


Figura 17. Modelo transacional de Tubbs

Fonte: TUBBS (2003; tradução do autor)

Outro ponto interessante da argumentação de Tubbs é a razão sobre a eficiência da comunicação, a saber:

$$R/S = 1$$

Se **S** representa o emissor ou a fonte da mensagem e **R** representa o receptor ou o destino da mensagem, a comunicação será completa e 100% efetiva quando a mensagem tanto no receptor quanto no emissor for igual. Além disso, Tubbs defende que a total efetividade da comunicação exige um clima psicológico positivo e de confiança.

A mediação ocorre quando nossas habilidades individuais naturais para criar, transmitir, receber e processar mensagens são estendidas, expandidas ou melhoradas tecnologicamente ou interpessoalmente (RUBEN, 1993). Sistemas de informação podem realizar a mediação de comunicações. Sacerdote e Fernandes (2013, p. 130) defendem que “os elementos sociais que se comunicam podem ser indivíduos, grupos, organizações ou quaisquer outros componentes da sociedade. As principais funções da comunicação

são: informar, instruir, comandar e influenciar".

A mediação da informação não é simplesmente a reprodução da mensagem entre emissor e receptor, nem uma entrega da mensagem de um polo a outro, seria uma transformação da comunicação na intenção de torná-la mais efetiva[11] (DAVALLON, 2003). O mediador pode atuar como conciliador – resolvendo conflitos de interpretação da mensagem –, facilitador – promovendo efetividade na comunicação –, bem como curador – garantindo que a mensagem não seja alterada, lida ou tenha sua autoria modificada sem autorização.

No que se refere a tecnologias, o termo mediação serve para escapar ao duplo determinismo social e técnico: a mediação é técnica no sentido do instrumento utilizado para estruturar a prática e social no sentido das formas de uso (DAVALLON, 2003). Schneier (2003) ensina que os sistemas tecnológicos também requerem mediadores e intérpretes. Para Davallon (2003), a noção de mediação parece designar as operações e seus efeitos no processo de comunicação (mediação técnica) e a intervenção da dimensão subjetiva nas práticas de comunicação (mediação social).

Segundo a teoria da mediação de Gumpert et al. (1990), a mediação é mais do que realizar o papel de canal na comunicação, ela envolve forças que influenciam o processamento humano da informação e molda interações sociais. O meio, nesse caso, torna-se parte do emissor e não apenas um canal para que a comunicação ocorra. O meio está inserido em um ambiente cultural, social e político. Nesse caso, o estudo do meio é também um estudo do ser humano, pois o meio torna-se uma extensão do ser humano.

Lombardi (2004) raciocina sobre as ideias de Dretske (1981), explicando o *informational link* com o uso da **Figura *18***, na qual uma fonte **S** está transmitindo informações para os receptores R_A e R_B através de algum canal físico. R_A e R_B são isolados uns dos outros no sentido de que não existe qualquer interação física entre eles. Mas Dretske considera que mesmo que R_A e R_B estejam fisicamente isolados existe uma *informational link,* relação informacional*,* entre eles. De acordo com Dretske, é correto dizer que há uma canal de comunicação entre R_A e R_B, porque é possível aprender algo sobre R_B olhando R_A e vice-versa. R_A contém informações sobre R_B e R_B sobre R_A.

Dretske, segundo Lombardi (2004), salienta o fato de que o correlações entre os

[11] Acredita-se que promover segurança da informação para as comunicações é tornar a comunicação mais efetiva. Muitas vezes o uso da criptografia, por exemplo, transforma as mensagens para protegê-las. Essas proteções procuram garantir que a informação não seja alterada, lida ou tenha sua autoria modificada sem autorização. Acredita-se que é nesse contexto que a segurança da informação contribui para a efetividade de comunicação.

eventos que ocorrem em ambos os receptores não é acidental, e sim funções de dependências econômicas comuns de R_A e R_B em S, por estarem consumindo as mesmas informações da mesma fonte. No entanto, para ele este é um exemplo de *informational link* entre dois pontos, apesar da ausência de um canal físico entre os pontos.

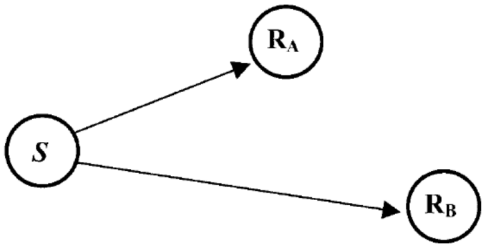


Figura 18. *Informational link*

Fonte: LOMBARDI (2004)

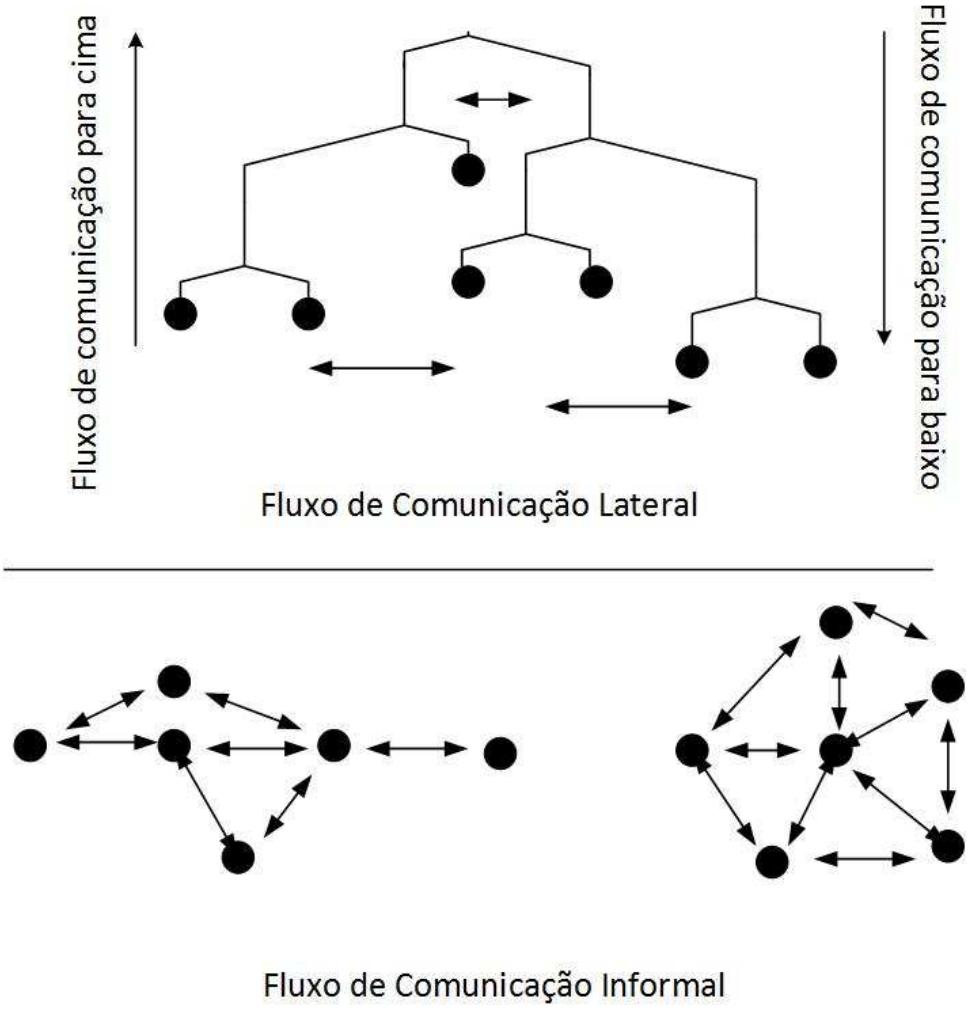


Figura 19. Rede com vários fluxos de informação

Fonte: BAKER (2002, p. 180; tradução do autor)

Para finalizar o referencial sobre comunicação e mediação serão apresentadas as ideias de Baker (2002). O autor defende que as mensagens trocadas no ambiente organizacional podem ser formais e informais. A estrutura formal de comunicação formal funciona por meio de regras, regulações, processos e é caracterizada por mais de um canal formal de comunicação. Por sua vez, a estrutura informal de comunicação é criada entre as pessoas em qualquer canal e direção e emerge do relacionamento interpessoal. Os dois tipos de comunicação se completam, e para o bom funcionamento de uma organização são necessários. A Figura 19 apresenta o modelo de comunicação de Baker.

Entretanto, segundo Silva e Ferreira (2007), os organogramas tendem a mudar mais lentamente do que as redes informais. Então, as comunicações informais são muito importantes para a adaptação da empresa às adversidades. Dessa forma, eles defendem que acompanhar as redes informais internas passa a ser um elemento relevante para os gerentes e os executivos.

Portanto, a comunicação e a mediação da informação são organizadas em modelos tendo em vista a efetividade da comunicação. A mediação observa o comportamento da comunicação e tenta intervir nela para auxiliar a efetividade dessa comunicação. A análise das comunicações utilizando modelos é interessante porque coloca em evidência os aspectos mais importantes e suprime partes que trazem uma complexidade, inerente à comunicação, desnecessária.

3.3 Segurança – ataque, alvo, vulnerabilidade – e a gestão de riscos da informação

A segurança da informação é uma disciplina muito estudada atualmente. Diversos autores procuram explicá-la, descrevê-la e exemplificá-la. Existe um mercado bilionário de produtos por trás desse conceito. Mas o que é, realmente, segurança da informação? É muito difícil entender-se a segurança de algo cuja definição é imprecisa, no caso, a informação.

Os eventos de segurança da informação, com a alta velocidade de difusão da informação e a expansão da complexidade tecnológica, podem dar causa a danos, diretamente proporcionais ao potencial adquirido pelos benefícios e pela dependência dessa tecnologia, tornando esses danos mais difíceis de serem detectados e reparados tempestivamente (SOUZA, 2011). Schneier (2003) defende que não há variação dos crimes ao longo da história, sejam eles cibernéticos ou não, ou seja, sempre existiram estelionatários, fraudadores, falsificadores, etc. A motivação e o objetivo da atividade “torta” continuam as mesmas, as ferramentas e as técnicas é que mudaram.

Entender o que é informação e descobrir seu diálogo com as demais ciências é o objeto de estudo da CI. O fato de se tratar de uma ciência interdisciplinar provavelmente lhe permite integrar o conceito de segurança em seu corpo de conhecimento. Nesse sentido, é necessário em primeiro lugar entender o que vem a ser segurança, em seguida integrá-la ao conceito de informação e com isso gerar um entendimento a respeito da segurança da informação. Para Fernandes (2010d, p. 15):

> O sujeito cognoscente é quem realiza o ato do conhecimento, enquanto o objeto é a coisa apreendida pelo sujeito. O nível ou extensão da apreensão do objeto pelo sujeito configura o problema da possibilidade do conhecimento, isto é, da apreensão completa da essência do objeto pelo sujeito. Sob o ponto de vista de uma teoria do conhecimento (epistemologia) para a segurança da informação, o seu elemento principal, a segurança, seria um fenômeno/conceito que se aplica na relação entre o sujeito e sua realidade.

Fernandes (2010d) diz que a informação consiste em um objeto manipulado por uma entidade viva, cognoscente, que permite a apreensão da realidade na qual se insere tal entidade. Para o autor, existe uma vinculação terminológica entre segurança da informação e CI, não apenas porque ambas contêm a palavra “informação”, e sim mais pela decorrência de que, sendo a informação um produto de natureza social, faz-se necessário reforçar o estudo dos fatores humanos na segurança da informação. Ele afirma que os vários modelos de organização da informação também são aplicáveis à organização da informação para a segurança, ressaltando que o conceito de risco introduz uma perspectiva dialética na construção de operações e processos de informação. Fernandes afirma ainda que dentre as contribuições que a segurança da informação pode introduzir na ciência da informação se destacam os conceitos de risco, identidade e individualidade.

A segurança da informação abarca diversos tipos de riscos, ameaças e ataques. Schneier (2003) define um ataque de segurança como uma ação específica intencional ou imprudente que atinge a segurança do sistema ou danifica um componente desse sistema. Para o autor, uma ameaça à segurança é uma potencial configuração de o atacante atingir a segurança.

Shostack e Stewart (2008) apresentam que uma ideia original sobre segurança da informação é que ela é primeiramente um problema de tecnologia e, portanto, a “solução” pode ser alcançada acumulando-se mais e mais tecnologia. Segundo os autores, não existem informações demonstrando que empresas que gastam mais com produtos de segurança necessariamente consigam uma redução nos incidentes de segurança da informação.

Mas, afinal, o que é segurança? Schneier (2003) define segurança como sendo tanto um sentimento quanto uma realidade. Assevera que estamos seguros quando nos sentimos seguros, livres de perigos e protegidos de ataques. Nesse sentido, segurança é apenas um estado mental.

Shostack e Stewart (2008) ensinam que a psicologia é outra ciência que podemos utilizar para entender melhor os desafios da segurança da informação. Por exemplo, muitas decisões, segundo eles, são tomadas com base no medo, e não em análise de risco. Os autores afiançam que a psicologia da compensação de risco, também conhecida como risco homeostático – que considera a aceitação do risco diretamente proporcional ao acréscimo da sensação de segurança –, é algo que precisa de atenção.

Contudo, para Schneier (2003) existe uma dimensão da segurança na realidade, e nessa dimensão não há nada a se fazer quando um incidente ocorre, não importa o que estamos sentindo. Na realidade estamos seguros quando estamos definitivamente resguardados. Nascimento (2008, p. 137) expõe:

> Nas décadas de 1950 e 1970, a grande preocupação com a segurança ficava limitada ao acesso físico a sistemas de computadores que ficavam confinados em espaços físicos organizacionais bem definidos. Na década de 1980, com o surgimento de microcomputadores e a possibilidade de comunicação em rede, até os dias atuais em que a conectividade e o compartilhamento de recursos, de tempo e da informação alcançaram níveis tão amplos, o foco da segurança da informação mudou, passando a ter uma abrangência muito mais ampla. Cumpre destacar que ao lado da evolução dos sistemas de informação e comunicação temos a evolução das relações políticas, governamentais, organizacionais, comerciais, por exemplo, para uma sociedade conectada, globalizada e altamente competitiva, onde as ameaças, os riscos e as vulnerabilidades de segurança aumentam exponencialmente tanto em número quanto nas formas de atuação.

É importante diferenciar segurança no sentido da proteção física (do inglês *safety*) de estabilidade, garantia ou certeza (do inglês *security*). A proteção é algo exógeno, ou seja, de fora para dentro. Por exemplo, caso a informação seja um objeto, realizar sua proteção seria aplicar mecanismos que salvaguardem o objeto, evitando que suas características físicas não sejam danificadas, destruídas ou mesmo que o objeto seja roubado. Schneier (1998) esclarece que o aspecto *safe* da segurança assume que o ataque é externo, que para esses casos são necessárias contramedidas de proteção.

Por sua vez, *secutity* pode ser entendida como a segurança no sentido de estabilidade, garantias ou certezas – endógena, eliminação de riscos. É o aspecto da segurança mantenedor do sistema em sua missão, sua razão de existir. Por exemplo, se

um sistema é desenvolvido para produzir determinada coisa e ao sofrer uma intervenção ele fica inabilitado para produzir essa coisa, sua segurança foi comprometida.

Shostack e Stewart (2008) informam que muito se fala em retorno de investimento em segurança para tentar criar confiança. Segundo os autores, a confiança pode ajudar uma empresa a vender seus produtos ou serviços. Eles apresentam a “segurança teatral”, que vem a ser uma medida de segurança puramente aparente. Essa segurança pode ser utilizada no sentido de manter uma marca com aparência de segurança, de se criar uma sensação de confiança.

Com relação à entrega de serviço computacional nas organizações, Avizienis, Laprie e Randell (2000) asseguram que confiabilidade é um atributo dentro da classificação de dependência. Para eles, confiabilidade é a medida de entrega contínua de um serviço correto. A confiança nesse serviço é uma questão relacionada à dependência que se tem dos elementos computacionais, assim se pode pensar em confiabilidade como a confiança em relação a algum produto ou serviço.

Schneier (1998) informa que as propriedades e os propósitos dos sistemas estão intimamente relacionados à segurança. Segundo Schneier (2003), segurança também é um sistema, um sistema de contramedidas e a interação entre elas. O autor relata que as catástrofes de segurança são extremamente raras. O que temos no cotidiano são pequenos incidentes que quando combinados podem gerar catástrofes. A segurança geralmente falha em suas junções – os pontos onde dois sistemas interagem. Há junções entre sistemas de segurança e outros sistemas e entre sistemas de segurança puramente. Essas falhas podem ser passivas e ativas:

- falhas passivas: o sistema falha em um ponto onde ele deveria agir;
- falha ativas: o sistema falha em um ponto onde ele não deveria agir.

Conforme Marciano (2006), uma vulnerabilidade representa um potencial ponto de falha, ou seja, um elemento passível de ser explorado por alguma ameaça. Avizienis et al. (2004) definem falha como a causa de um serviço não ser devidamente entregue, e isso gera um erro. Para os autores, a vulnerabilidade é uma falha interna que habilita a ocorrência de um erro. Muitos dos controles de segurança da informação detectam erros e executam respostas. Segundo Avizienis et al. (2004), a exploração de vulnerabilidades é uma ação maliciosa para gerar uma falha ou erro.

Schneier (2003) afirma que sistemas de segurança são úteis precisamente pelo que

eles não permitem que ocorra. A engenharia de sistemas envolve, sobretudo, fazer os sistemas funcionarem. No caso da engenharia de segurança seria fazer com que os sistemas não falhem. Na detecção de falhas há o problema de se prover um controle que gere muitos alertas falsos: mesmo não havendo erros ocorre um alerta.

Schneier (2003), segurança é, geralmente, uma questão de prevenção aleatória sobre consequências de ações intencionais, imprudentes ou despreocupadas de outros sobre determinado contexto, ou seja, segurança, nesse sentido, está mais ligada à prevenção, ao controle – mesmo que ele possa falhar também.

Em muitos casos, os custos e os benefícios da segurança são subjetivos. Schneier (2003) refere que a tecnologia geralmente facilita as ações das pessoas. A segurança é justamente o contrário: ela tenta prever a ocorrência de algo ou que alguém irá fazer algo – na intenção de determinar que se está tentando burlá-la.

A segurança é um eterno perde-e-ganha (*trade-off*), segundo Schneier (2012). Quando se aplica segurança, por um lado acrescentam-se melhoramentos, mas por outro se retiram conveniências. Na **Figura *20*** a pirâmide representa a relação entre a segurança e as conveniências da funcionalidade e da utilidade. Quando se ganha em segurança se perde nessas duas categorias.

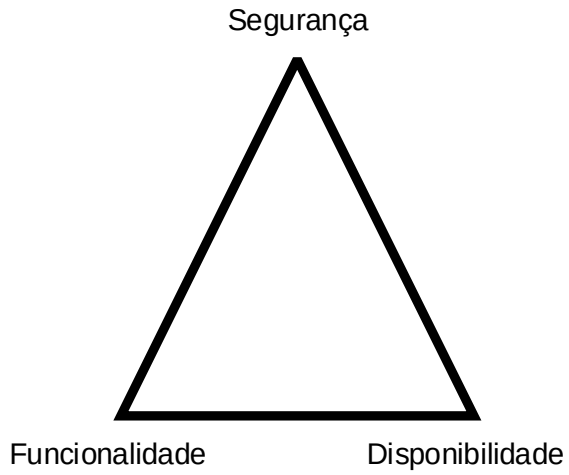


Figura 20. Modelo do perde-e-ganha entre segurança, da funcionalide e da utilidade
Fonte: WATSON; MASON; ACKROYD (2014; tradução do autor)

Para Schneier (2012), os sistemas de segurança são a última camada de amparo e a mais escalável. Ele diz ainda que os mecanismos de segurança podem ser classificados como:

- defesa – detêm ou atrasam a ameaça;

- intervenção – agem no momento do ataque, detectam o problema e tentam solucioná-lo tempestivamente;
- sistema de detecção/resposta – detectam e executam uma resposta programada, geralmente não intervindo no ataque;
- sistema de auditoria/forense – geralmente ocorrem levantando informações para a prevenção e a investigação sobre um ataque.
- sistema de recuperação – recuperação para um estado aceitável após um ataque;
- intervenção preemptiva – operam antes do ataque e imediatamente depois de uma detecção de risco.

Shostack e Stewart (2008) afirmam que ameaças à segurança e vulnerabilidades sempre existirão. Schneier (2003) afiança que um ataque de segurança é uma ação específica intencional ou imprudente que atinge a segurança do sistema ou danifica um componente desse sistema. Para o autor, uma ameaça à segurança é um potencial meio de o atacante atingir a segurança.

A segurança eficiente é um encadeamento de contramedidas, mas não se trata do número de contramedidas. Quando uma contramedida falha outra deve atuar, elas devem ser independentes, porém interconectadas. A compartimentação é excelente para impedir que uma falha implique outra falha. As contramedidas testadas e validadas são muito melhores que as novas e não testadas, especialmente com tecnologias complexas (SCHNEIER, 2003).

Schneier (1998) defende que a complexidade é o pior inimigo da segurança. O autor garante que a segurança é complexa, porém pode ser quebrada com simples e poucos passos. Então, como projetar e executar uma boa segurança, de forma simples? Para uma segurança eficaz e de sucesso, Schneier (2003) determina cinco questões a serem respondidas:

1. O que está sendo protegido?
2. Quais os riscos a que se está sendo submetido?
3. O quanto a segurança pode mitigar os riscos a que se está sendo submetido?
4. Quais os riscos e os efeitos colaterais as contramedidas de segurança incluem no processo?
5. Quais os custos e os benefícios que as soluções de segurança proporcionam?

É no sentido de se encontrar a segurança eficaz que grupos se reúnem para construir modelos de comportamento obrigatório no tema. Na esfera dos estudos sobre a segurança da informação é indispensável mencionar a família de normas 27000 da Associação Brasileira de Normas Técnicas (ABNT). Souza (2011) diz que as normas da ABNT são basicamente um conjunto de padrões para se criar um Sistema de Gestão da Segurança da Informação. Esse sistema seria um processo contínuo de planejamento, execução, controle e ajuste. Para Avizienis et al. (2004), segurança da informação é a concorrente existência de: a) disponibilidade apenas para usuários autorizados, b) confidencialidade e c) integridade contra significado impróprio não autorizado.

Em outras palavras, a confidencialidade é a propriedade de a informação não estar disponível ou revelada a indivíduos, entidades ou processos não autorizados; a integridade é a propriedade de salvaguarda da exatidão e da completeza da informação; e a disponibilidade é a propriedade de a informação estar acessível e utilizável, sob demanda, por uma entidade autorizada (ABNT, 2006).

Fernandes (2010d) explica que as definições de disponibilidade e integridade só podem ser interpretadas em um contexto no qual existem usuários e recursos informacionais a serem recuperados. Acerca dos recursos, o autor indica que as principais qualidades da segurança, pelo menos do ponto de vista normativo, são concernentes à busca por integridade, disponibilidade e confidencialidade, sendo comuns, no entanto, o uso de outros conceitos, como autenticidade e não repúdio. Para Rezende (2011, p. 8),

> [...] é certo que existem contextos onde os mesmos dados e ao mesmo tempo o interesse de um lado na comunicação demanda sigilo enquanto o outro lado demanda transparência, e desses dados, nenhum interessado é mais “legítimo dono” do que o outro. Ante a escolha de mecanismos de segurança, as condições necessárias para que o uso dos mesmos seja eficaz são as premissas de confiança.

Marciano (2006), pela ótica da teoria das ciências sociais, garante que o foco da segurança da informação é que a informação gerada, armazenada, tratada e transmitida seja comunicada, sendo a comunicação um processo grupal tanto interno como externo ao meio organizacional. Para Marciano, os ativos da informação são os indivíduos, os componentes tecnológicos e os processos envolvidos em alguma etapa do ciclo de vida da informação, a saber, sua origem, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização.

Vale lembrar-se do que Capurro e Hjørland (2003) trouxeram: apresentaram a informação como elemento da comunicação e como parte dos modelos mentais. A

contribuição de Marciano é no sentido de estender a segurança a todos os ativos informacionais, aqueles que agem sobre a informação. Mas é importante mencionar que os passivos da informação – documentos, modelos, ou seja, artefatos da informação – também merecem a atenção da segurança da informação.

A segurança dos ativos informacionais é uma necessidade corporativa. Esses ativos podem ser dimensionados em três esferas principais: as pessoas, os processos organizacionais e as tecnologias (ALMEIDA; CARNEIRO, 2013).

Fernandes (2010d) afirma que a segurança da informação é uma área da atividade humana cujas bases epistemológicas ainda não foram descobertas, mas possui uma práxis relevante. Este autor defende que a TI constitui o ponto de onde se evidenciou a importância da segurança da informação como é hoje praticada, e seguramente permanecerá tendo papel de suma importância no avanço da prática coesa com a ciência da informação. Ele doutrina, ainda, que o pretenso objeto de preservação da segurança da informação é, pelo menos da forma prescrita, a própria informação ou o conceito que dela fazem seus praticantes. É interessante entender que o objeto informação não pode prescindir de íntima relação com o sujeito que a alcança, e que se o conceito de informação não está claro para os que a praticam, muito menos estará o da segurança da informação.

A administração e o controle da segurança, para Godinez et al. (2010, p. 54), relacionados à informação organizacional procuram garantir que a informação não tenha sido corrompida, destruída ou usada de forma inescrupulosa. Schneier (2003) esclarece que a segurança é uma questão de prevenção adversa sobre consequências de ações intencionais ou imprudentes de outros sobre determinado contexto.

Quando se fala em fluxo da informação em relação aos processos de gestão da informação, uma questão a ser definida é a segurança, tendo como contexto uma sociedade globalizada e caracterizada pela competitividade (NASCIMENTO, 2008). Nascimento afirma que a segurança é um desafio da arquitetura da informação, da organização da informação, e que os autores que desenvolvem ou utilizam as técnicas, as práticas e as metodologias da segurança da informação em sua maioria não consideram os fundamentos da Ciência da Informação. Conforme Marciano e Lima-Marques (2006, p. 89):

> O uso cada vez mais disseminado de sistemas informatizados integrados por meio de redes é um fato determinante da sociedade da informação. Este universo de conteúdos e continentes digitais está sujeito a várias ameaças que comprometem seriamente a segurança do complexo usuário-sistema-informação. A tecnologia da

> informação é capaz de apresentar parte da solução a este problema, mas não é capaz de resolvê-lo integralmente.

Para Fernandes (2010d, p. 20),

> Dado que a segurança da informação alcançou evidência no seio da tecnologia e de sua exposição ao meio de comunicação aberto que é a internet, as atuais organizações que prestam serviços de informação com segurança são tipicamente aquelas que empregam tecnologia computacional, as chamadas organizações de TI.

A segurança da informação e comunicações (SIC) é hoje mais complexa e automatizada que suas precursoras, e sua finalidade é incrementar a eficiência operacional e gerencial dos processos de trabalho, de produção, de prestação de serviços e de efetivação dos negócios. As abordagens “de gestão” da segurança da informação estendem-se às de segurança computacional tecnológica, assim como prega Fernandes (2010c).

Ao se pensar em segurança da informação é preciso considerar também o conteúdo das informações trabalhadas, pois somente assim poderia ser escolhida uma segurança adequada (NASCIMENTO, 2008). Nascimento afirma que “a segurança da informação está associada às chamadas ‘metodologias *hard*’, de implantação e controle mais objetivos e que envolvem ações sistematizadas, na maioria das vezes associadas a tecnologias da informação.” Nessa linha, Rezende (2011, p. 18) assegura:

> Tendo entendido que com tecnologia apenas não há solução, as estratégias de segurança da informação passam então a atuar em processos normativos: licenças, atos administrativos, leis e tratados internacionais. Porém, tais estratégias agravam interações e conflitos de interesses porque incorporam mais riscos ao sistema de segurança da informação, atuando em querelas que antes a tecnologia não participava.

Para Fernandes (2010d), a finalidade da gestão da segurança da informação não se restringe apenas à promoção e à manutenção da integridade, da confidencialidade e da disponibilidade como propriedades fundamentais da informação. Ela busca a garantia da satisfação das necessidades de informação dos usuários que colaboram para a concretização das atividades organizacionais, em obediência às condições ambientais e regulatórias. Para isso, pode-se pensar que é preciso se estabelecer um modelo de comportamento no uso da informação, geralmente institucionalizado por meio da política

de segurança da informação.

A formalização de uma política de segurança da informação ou, de forma mais ampla, uma política para o uso da informação na organização é condição essencial para nortear todas as atividades nas quais se insere a segurança (FERNANDES, 2010d).

Gulati (2003) ensina que uma política de segurança da informação bem documentada e de fácil acesso é um guia fundamental para uma boa estratégia de segurança. Segundo ele, essa política deveria deixar bem claro os termos do comportamento seguro e especificar o que deve ser seguido para se estar de acordo com os preceitos da segurança organizacional. Como defende esse mesmo autor, a segurança da informação é essencial para a manutenção de qualquer organização no mercado.

Consoante Fernandes (2010d), considera-se a segurança da informação uma matéria multidisciplinar, pois facilmente se verificam inter-relações entre ela e quase todas as áreas do conhecimento humano, tais como economia, educação, engenharia, história, leis, linguística, filosofia, ética, ciência política, psicologia, metodologia de pesquisa, semiótica, antropologia, comunicação, ciência da computação, sociologia. Porém, Fernandes alerta que não encontrou estudos que correlacionassem segurança com arte, justificando essa constatação com o fato de a segurança ser uma possível antítese do caos e da liberdade, situações geralmente ligadas à arte.

A vanguarda da segurança da informação tem contribuído sobremaneira com seu objeto de estudo ao usar métodos científicos para analisar o mundo real numa tentativa de solucionar problemas relevantes de segurança, conforme Shostack e Stewart (2008). Os autores explicam por que o profissional de segurança precisa atualmente utilizar uma abordagem interdisciplinar, estudando economia, psicologia, engenharia, operações, sociologia e a Teoria dos Jogos.

Na ABNT (2005, p. 2) encontra-se que um evento de segurança da informação pode ser definido como um caso concreto de um sistema, serviço ou rede, com uma provável violação da política de segurança da informação ou falha de controles e contramedidas, ou uma circunstância de antemão ignorada, importante para a segurança da informação. Por sua vez, um incidente de segurança da informação é identificado por um conjunto de eventos indesejáveis e imprevistos que tenham uma grande probabilidade de afetar as operações do negócio e de ameaçar a segurança da informação.

Imagine-se que a polícia prendeu duas pessoas: Fulano e Cicrano. A polícia deseja desvendar um crime que envolveu esses dois presos. Todavia, ela precisa da confissão dos presos, pois não há provas suficientes para incriminar qualquer um deles. Então os presos

se encontram na seguinte situação: a polícia oferece a benesse da delação premiada – quem confessar o que realmente ocorreu, incriminando o outro bandido, terá redução da pena. A pena máxima para o crime é de dez anos. Trabalhando as possibilidades, pode-se ter: se um preso testemunhar contra o outro e o outro não testemunhar contra ele, este terá a pena reduzida a dois anos e o outro ficará dez anos preso, e vice-versa; se eles testemunharem um contra o outro, ambos irão para a cadeia por dois anos. Se ambos mantiverem o silêncio, serão liberados da cadeia. Isso é conhecido como o dilema do prisioneiro da Teoria dos Jogos. Para Schneier (2012), o dilema do prisioneiro é um tipo de dilema social, e os dilemas sociais são as situações que geralmente demandam segurança.

Por trás dos dilemas individuais, Schneier demonstra como o comércio, por exemplo, age similarmente ao dilema do prisioneiro, e essa atuação está intimamente ligada aos mecanismos de confiança. É dessa forma que a segurança pode ser definida: tanto pelo sentimento individual e coletivo de proteção em determinado contexto como pela engenharia de produtos. Imagine-se outra situação: duas pessoas trocam maletas fechadas. Uma dessas pessoas está interessada em uma maleta de dinheiro, e a outra em uma maleta com mercadorias. A semelhança dessa situação com o dilema do prisioneiro é que nessa troca um dos envolvidos pode simplesmente entregar uma maleta fazia, ou mesmo com qualquer outra coisa em vez da mercadoria desejada pela outra parte. Isso também ocorre no comércio eletrônico: transações às cegas e remotas.

Schneier (2012) preconiza que a segurança é o que se precisa quando não se tem confiança. Segurança é, para o autor, definitivamente a forma de introduzir confiança na sociedade, além de reduzir o risco a níveis toleráveis, permitindo que a confiança participe do processo em questão ao preencher as lacunas. Claro que o grau de liberdade do sistema, ou o processo, é afetado, podendo suas funcionalidades serem limitadas, assim como sua utilidade. Mais à frente serão analisados a confiança e o risco.

Shostack e Stewart (2008) defendem que a indústria da segurança tem conflitos de interesse, e essa constatação explica a existência de diversos problemas de segurança. Essa visão dos autores e o que Schneier apresenta sobre dilemas sociais remetem aos conflitos de interesse presentes no modelo da Figura 21, retirado de Schneier (2012). A Figura 21 representa os conflitos de interesse no contexto de um indivíduo na sociedade, a saber: conflitos de interesses egoístas, de interesses sobre determinações morais, de interesses relacionais, de interesses de autodefesa e de interesses egocêntricos. Podem-se observar diversas pressões ou forças sociais interagindo no indivíduo enquanto ele está inserido em seus grupos sociais, e, nesse contexto, nem sempre há plena segurança, isso

leva o indivíduo a um estado de confiança em algo ou alguém ou de abuso da confiança de alguém para satisfazer seu interesse.

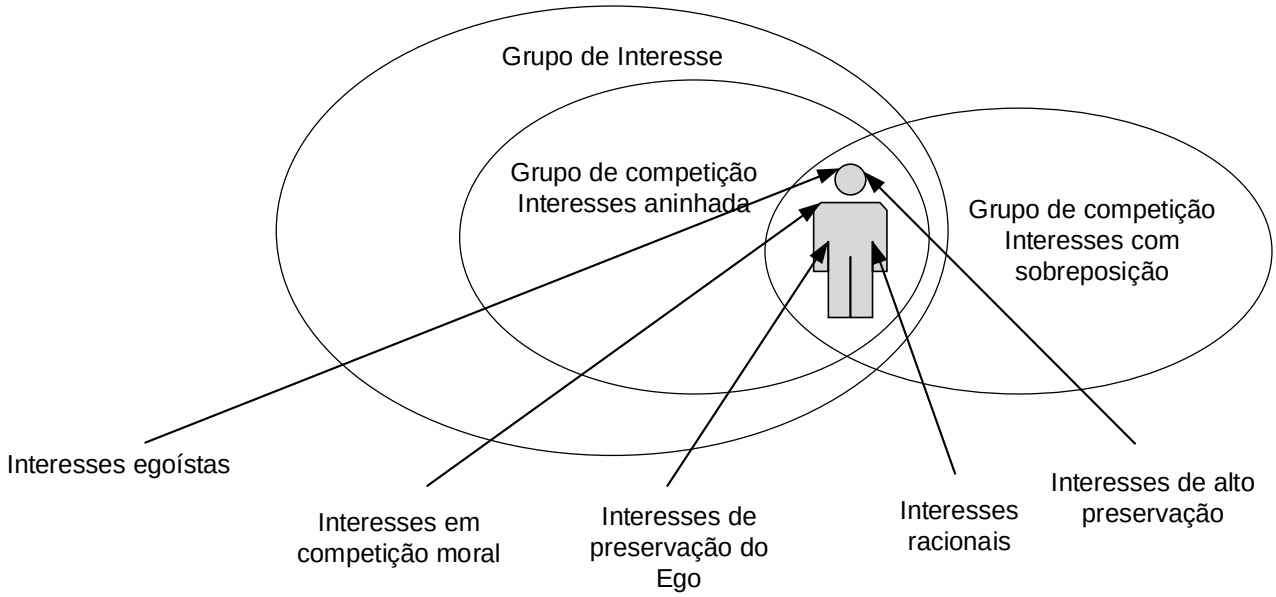


Figura 21. Disposição dos conflitos de interesse sobre um indivíduo

Fonte: SCHNEIER (2012, p. 141; tradução do autor)

Conseguir confiabilidade no espaço virtual tem sido um desafio, porque as técnicas de ataque e de defesa se desenvolvem paralelamente, e a TI está em um movimento de convergência e dispersão, portanto as possibilidades de conflitos de interesse aumentam. Conflitos aumentam entre os que desenvolvem, fornecem ou usam tecnologias, os que precisam de proteção contra mediações indevidas, os que competem por um desses objetivos, além dos que agem com fins ou por meios escusos. Aqui é onde os conflitos se tornam mais decisivos para o processo da segurança, a começar pela influência em estabelecer o que seja restringível, balizado no que seria indevido ou hostil por um ou outro interesse. Essa restrição pode ser técnica, institucional ou legal, e ela é totalmente influenciada por métodos de coerção, graus de prioridade, rigor e eficácia restritiva do mecanismo elegido para tal (REZENDE; 2011). Rezende (2011, p. 2) afiança:

> Em toda civilização, regras de comportamento (costumes, normas, leis) são estabelecidas, escritas ou subentendidas, para dar segurança (estabilidade, previsibilidade) às práticas sociais. Entende-se por práticas sociais as relações interpessoais, institucionais, de negócio, de produção, etc. Não há segurança sem regras, e isso se manifesta nos valores de uma cultura, nela possibilitando laços de compromisso e responsabilização. Assim as sociedades complexas se formam e evoluem: com base em engajamento coletivo nessas práticas, em entendimento e aceitação desses laços, e em métodos coercitivos para inibir transgressões.

> Métodos esses geralmente operados ou sancionados pelo Estado, mas nem sempre. De qualquer forma, seja de onde venha a sanção coercitiva, a coesão social baseia-se em confiança coletiva na eficácia dessas práticas, laços e métodos.

Schneier (2003) ensina que a segurança de pessoas se resume basicamente ao desenvolvimento e à execução de protocolos. Se não há sujeito a ser atacado, não há problema de segurança. Os protocolos de segurança são séries de passos que pessoas confiáveis devem executar, os passos são desenhados para fortalecer as regras de segurança. Os protocolos são simples e servem para mitigar potenciais abusos de confiança. É claro que os protocolos introduzem mais riscos, como qualquer contramedida, por isso devem ser cuidadosamente analisados e desenhados.

Por sua vez, como define Schneier, os procedimentos são passos que as pessoas confiáveis devem executar. Por essência, os procedimentos de segurança são executados quando algo deu errado. Eles são os passos a serem executados quando um evento de segurança ocorreu. Protocolos são rotinas que as pessoas seguem no dia a dia, os procedimentos são as repostas às anomalias.

Watson, Mason e Ackroyd (2014) asseguram que as pessoas não podem simplesmente ouvir falar sobre engenharia social e decidir que não serão mais vítimas de golpes. Como Schneier (2012) defendeu, é preciso um trabalho sistemático de conscientização, construção de protocolos, procedimentos, treinamentos, simulados, etc. Normas como, por exemplo, a de controle de acesso por necessidade de saber – aquela normalizadora do controle de acesso à informação a quem necessita conhecê-la para a execução do seu trabalho –, são muito importantes para ordenar o ambiente informacional.

Watson, Mason e Ackroyd (2014) afirmam que a seleção do alvo pode seguir a pirâmide da **Figura *22***. Por meio do modelo desses pesquisadores pode-se depreender que é preciso uma cuidadosa escolha de características e informações sobre o alvo antes de selecioná-lo. Observa-se que são diversas etapas sistemáticas de um aprofundamento de informações sobre a possível vítima.

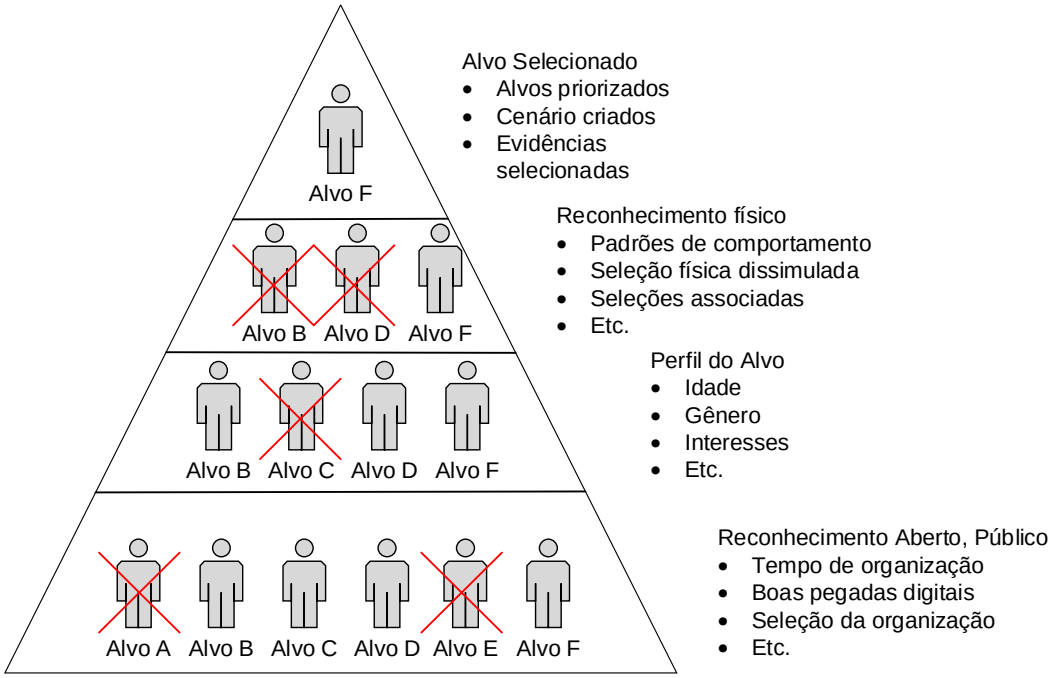


Figura 22. Pirâmide de seleção do alvo

Fonte: WATSON; MASON; ACKROYD (2014)

Basicamente um ataque se configura com a localização do alvo, a seleção da vulnerabilidade a explorar, a seleção da técnica de exploração da vulnerabilidade, testes de ataque, o ataque inicial, a elevação do privilégio – lê-se acesso privilegiado – e a eliminação dos rastros.

Ressler (2006) classifica os analistas de redes sociais em dois grupos: os coletores de dados e os modeladores. Segundo ele, a coleta de dados para a análise de redes sociais é uma tarefa árdua, também afirma que os complexos modelos criados na análise de redes sociais estão sendo gerados para oferecer *insights* em diversas aplicações, principalmente em segurança. Portanto, lidar com ARS e confiança é uma tarefa penosa, e em determinados trabalhos será preciso inteligência.

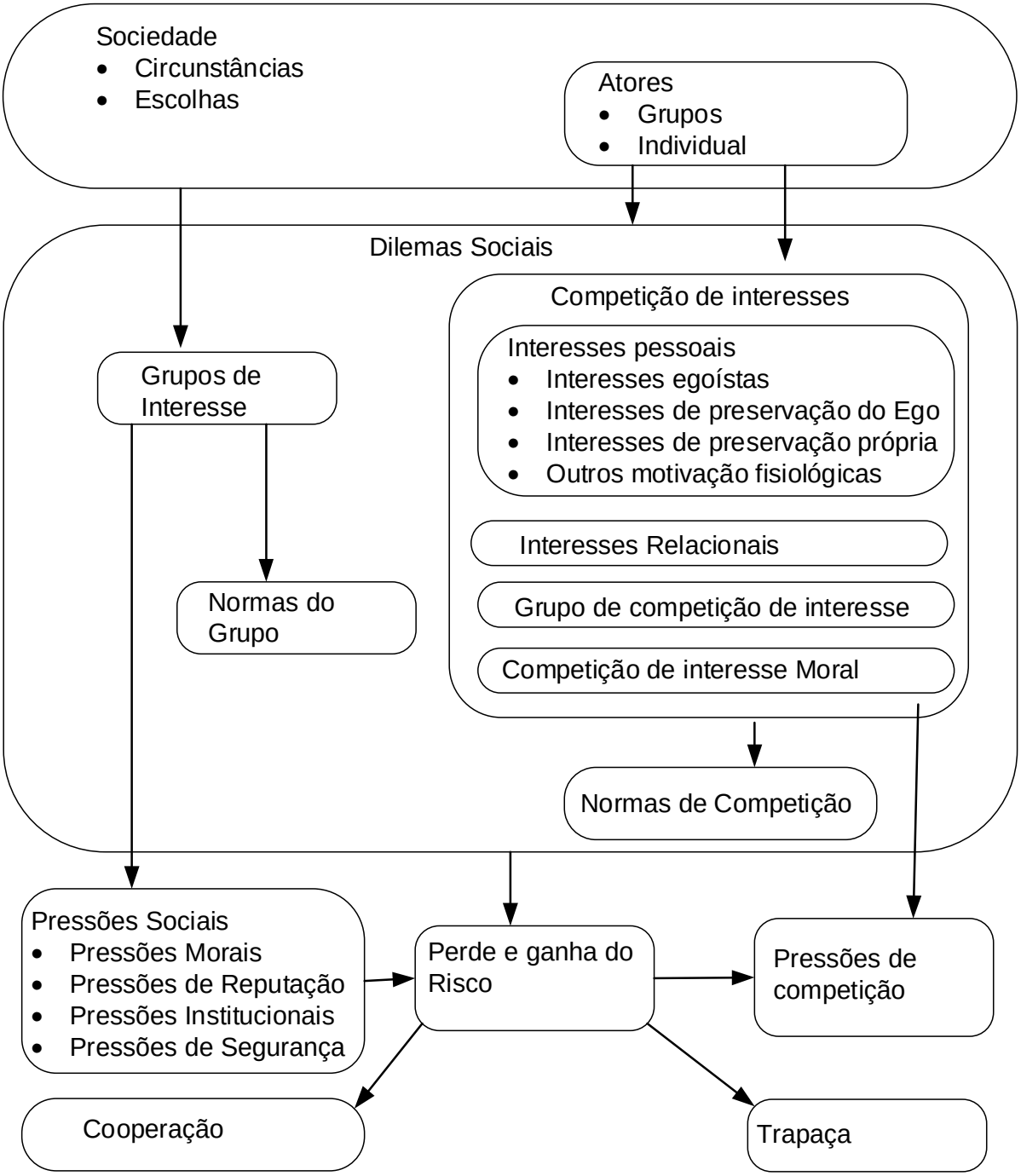


Figura 23. Mapa conceitual entre sociedade, dilemas sociais e pressões sociais

Fonte: SCHNEIER (2012; tradução do autor)

Como pode ser percebido na **Figura *23***, a sociedade, seus grupos e atores sofrem constantemente pressões sociais e estão envolvidos em competições e dilemas. O perde-ganha da segurança da informação está diretamente ligado às situações de competição. Assim, muitas vezes é impossível aplicar certos controles devido aos conflitos de interesse e às pressões sociais. Por meio de normas, modelos de comportamento obrigatório, contramedidas de segurança e do estabelecimento de confiança são moldados e

estabelecidos os sistemas de gestão de segurança da informação. A partir desse estabelecimento as pressões sociais e os riscos situacionais são contornados. Ao fim e ao cabo, os cenários de segurança da informação se resumem a momentos de cooperação e trapaça nos quais os controles de segurança irão prever, detectar e responder a incidentes.

Watson, Mason e Ackroyd (2014) afirmam ser verdadeiramente fascinante a quantidade de informação colocada em domínio público, mas também é assustador que as organizações não saibam o que estão realmente divulgando.

Por fim, destaque-se a importância de se observar o comportamento dos *hackers*, que quebram as regras julgadas estúpidas por eles para chegar aos resultados que consideram melhores, ou seja, *outliers*, na visão de Schneier (2012), “o ponto fora da curva”, aqueles que não aceitam as pressões sociais e agem de acordo com seus ideais, seu desejo, sua conveniência e seu egoísmo. Essa observação seria importante para gerenciar os riscos de segurança.

Conclui-se que é pela exploração das vulnerabilidades que o malicioso se manifesta e se beneficia, corroborando Avizienis et al. (2004), que defendem que os complexos problemas da interação homem-máquina (incluindo a interface do usuário) agravam o desafio: o lado obscuro da natureza humana nos provoca a tentar antecipar novas formas de comportamentos maliciosos, que levam a mais formas de falhas maliciosas, requerendo novas defesas.

3.4 Engenharia social

As comunicações podem ser pensadas com o objetivo de controlar e influenciar as pessoas (BERLO, 2003; SACERDOTE; FERNANDES, 2013; CAPURRO, 1992). Mitnick e Simon (2002) definem a engenharia social como a arte ou a ciência de influenciar ou enganar as pessoas. Na engenharia social, para os autores, o atacante, com o auxílio de informações privilegiadas obtidas por diversos meios escusos, engana as pessoas para obter informações valiosas para ele ou para terceiros. Esses ataques são executados por espiões industriais, detetives particulares, estelionatários, etc. Mitnick e Simon (2002, p. 15) alertam:

> Mas na verdade a invasão da segurança de uma empresa quase sempre começa com o cara mau obtendo alguma informação ou algum documento que parece ser muito inocente, tão comum e sem importância que a maioria das pessoas da organização não vê nenhum motivo pelo qual ela deva ser protegida e classificada.

Schneier (2012) esclarece que existem muitas pesquisas na detecção de fraudes, estelionato, trapaças, e a conclusão a que se chega é que o ser humano não é eficiente na detecção desses problemas. Para o autor há exceções, mas em geral existe um alto risco de se chamar enganosamente de mentirosos aqueles que são verdadeiros e vice-versa. Ele afirma ainda que a sociedade sempre pensa ser melhor em detectar esse tipo de situação do que na verdade é.

Hadnagy (2011) faz uma reflexão sobre uma série de definições para a engenharia social. O autor informa que ela seria a ação quando uma pessoa mente para obter alguma informação, que ela seria a ação de ser um bom ator ou seria o conhecimento de saber como pegar coisas grátis. Hadnagy, ao criar sua própria definição, divide o termo engenharia social em duas partes: engenharia e social. Social seria a capacidade do ser humano de se relacionar em comunidade, e a engenharia, a arte ou ciência de aplicar o conhecimento científico puro aos problemas cotidianos. Portanto, engenharia social seria a arte ou ciência de se aplicar conhecimento científico puro aos problemas cotidianos dos relacionamentos em comunidade do ser humano. A engenharia social leva o ser humano a tomar certas atitudes, a agir, a servir a um propósito que vai além da percepção do agente. Watson, Mason e Ackroyd (2014) apresentam definições para a engenharia social:

- A aplicação de princípios da sociologia para resolver problemas sociais específicos.
- A arte de manipular intencionalmente o comportamento de alguém utilizando técnicas de comunicação especialmente construídas.

- A arte de utilizar o comportamento humano para quebrar a segurança sem efetivamente participar das ações.
- A arte de levantar informações sensíveis e manipular indivíduos a executar ações para obter resultados sobre as quebras de segurança.

Para Gulati (2003), a engenharia social é a arte de utilizar o relacionamento entre pessoas para quebrar a segurança sem que a vítima perceba que está sendo manipulada. Ele divide a engenharia social em duas categorias:

1. fraudes baseadas em tecnologia;
2. trapaças baseadas puramente em relacionamento humano.

Schneier (2003) define engenharia social como a ação de enganar pessoas se passando por alguém que realmente não se é; é o ato de conseguir ajuda involuntária de alguém dentro de uma organização. Geralmente conhecer a cultura organizacional – por exemplo, jargões e gírias internas – influencia e facilita as ações desse tipo. Segundo o autor, a engenharia social nada mais é que uma fraude, mas a tecnologia a ajuda e lhe confere certo *glamour*. Por exemplo: alguém ao telefone se faz passar por um técnico do suporte e consegue acesso remoto a uma organização.

Dolan (2004) afirma que não é uma questão do quanto se conhece, mas sim quem você conhece. O autor sustenta que em muitas situações conhecer a pessoa certa é uma vantagem competitiva, seja no trabalho seja em outras situações sociais. Mais ainda, conhecer a pessoa certa, segundo Dolan, é engenharia social. Assim, ele define engenharia social como a habilidade de utilizar os relacionamentos sociais para atingir objetivos.

Um ponto de convergência de todas as definições de engenharia social apresentadas até aqui seria que o engenheiro social (eng. s.) não passa de um golpista, de um aproveitador, que se vale dos relacionamentos, da comunicação e de outras ferramentas tecnológicas para enganar e ludibriar os bem intencionados. Segundo Gulati (2003), existem técnicas comuns de engenharia social, são elas:

- **acesso direto** – quando não há intermediário entre o atacante e a vítima, sendo o contato direto, podendo ser pessoalmente;
- **garimpagem de informações descartadas** – o atacante procura informações úteis para sua ação onde as vítimas as descartaram julgando serem lixo;

- **escutas** – o atacante instala algum mecanismo para gravar as comunicações da vítima;
- **uso da boa-fé de técnicos especialistas** – o atacante se passa por uma pessoa que necessita de suporte técnico, porém na verdade utilizará os conhecimentos do experiente para tirar proveito;
- **passar-se por um técnico** – o atacante se passa por um técnico de suporte para enganar a vítima e obter informações;
- **abuso do autoritarismo** – o atacante se passa por um superior e utiliza conduta imperativa para solicitar informações à vítima;
- **cavalos de Troia** – o atacante utiliza um *software* camuflado por outro *software* para colher informações;
- **janelas *popup* –** o atacante injeta janelas *pop-up* para confundir a vítima e fazê-la agir de forma displicente.

Dolan (2004) informa que os engenheiros sociais usam as seguintes táticas:

- alavancagem de confiança;
- falsificação de sua utilidade;
- verificação de antecedentes, levantamento de informações;
- tentativas de conhecer os processos internos;
- tentativas de imitar a autoridade;
- utilização da tecnologia.

Essas táticas de Dolan podem ser usadas de forma combinada para se atingir os objetivos. Ele diz que os engenheiros sociais utilizam ataques divididos em etapas para atingir objetivos maliciosos gradativamente. Para o autor, a natureza humana é a maior vulnerabilidade a ser explorada pelo engenheiro social, pois as pessoas geralmente confiam facilmente e obtêm satisfação em ajudar os necessitados.

Silva (2012, p. 2) constata que, usualmente, “o principal recurso para exploração de informações utilizando engenharia social é a utilização de conhecidas tendências, falhas ou brechas psicológicas, sociais e comportamentais”, sendo as mais utilizadas:

> **Vaidade (pessoal ou profissional)**: há maior receptividade à avaliação positiva e favorável que coincida com interesses e objetivos pessoais. Assim, a identificação com argumentos concordantes com a avaliação pessoal ou profissional gera aceitação espontânea.

> **Autoconfiança**: é intrínseca a vontade de se transmitir em diálogos o ato de fazer algo bem (mostrar-se bom em determinado assunto, área ou habilidade), coletivamente ou individualmente, procurando transmitir segurança, conhecimento, saber e eficiência, objetivando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou indivíduo.
>
> **Formação profissional**: é permanente a busca pela valorização da formação e habilidades adquiridas, demonstrando domínio na comunicação, execução ou apresentação, almejando o reconhecimento pessoal inconscientemente em primeiro plano.
>
> **Vontade de ser útil**: é bem-visto agir com cortesia, bem como ajudar outros quando necessário.
>
> **Busca por novas amizades**: é nato sentir-se bem quando elogiado, criando-se um estreitamento afetuoso e a sensação de intimidade, tornando o "alvo" mais vulnerável e aberto a ceder informações.
>
> **Propagação de responsabilidade**: o compartilhamento do encargo traz a sensação de conforto, de que não se está sozinho na busca da solução do que foi proposto.
>
> **Persuasão**: é possível obter dados específicos de forma indireta, identificando características comportamentais que tornam as pessoas vulneráveis à manipulação através de uma considerável quantidade de técnicas disponíveis a qualquer pessoa que tenha interesse em adquiri-las.

Watson, Mason e Ackroyd (2014) asseguram que a confiança é uma situação social que pode ser explorada por um engenheiro social para obter determinada informação. Afirmam que com as técnicas adequadas é possível invocar a confiança de qualquer pessoa, assim como qualquer outro sentimento, por exemplo, raiva, benevolência, pena, etc.

Gragg (2002) expõe que existem diversos gatilhos psicológicos que fazem a engenharia social tão bem-sucedida. Esses gatilhos incluem: forte afeto, sobrecarga de trabalho, reciprocidade, relacionamentos falsos, difusão de responsabilidade e dever moral, autoridade, integridade e consistência.

Para Turner (2005), os ataques de engenharia social podem ser comportamentais ou psicológicos. Táticas de ataque comportamental poderiam ser vasculhar o lixo, "olhar sobre o ombro" ou aprender sobre a empresa lendo documentos públicos. Táticas psicológicas podem ser consideradas "*hacking* de pessoas" ou a exploração do fator humano. Turner afirma que o engenheiro social explora os comportamentos humanos, como confiança, presteza, ignorância, para conseguir violações de segurança. As pessoas desejam confiar umas nas outras, e essa confiança pode ocorrer mesmo sem uma boa razão. Segundo o autor, toda pessoa honesta geralmente assume que os outros estão

igualmente bem-intencionados. Mitnick e Simon (2002) afirmam que:

> [...] a confiança das pessoas pode ser usada de forma errada se for manipulada de determinadas maneiras. Uma dessas técnicas comuns envolve a criação de uma sensação de confiança por parte de uma vítima. Após conseguir a sua confiança, a ponte levadiça é abaixada e o portão do castelo se abre para que ele entre e obtenha as informações desejadas.

Silva (2012, p. 1) define engenharia social como “o termo utilizado para identificar um conjunto de técnicas cujo objetivo é a obtenção de informações relevantes a respeito de um determinado indivíduo ou organização”. As informações são provenientes quase sempre de pessoas próximas ao alvo ou do próprio sem que ele saiba. O termo engenharia social pode ser encarado como sinônimo de espionagem. As informações podem ser obtidas utilizando-se a ingenuidade ou a confiança da vítima, persuasão, dissimulação.

Segundo Dolan (2004), a engenharia social pode ser aplicada de forma revertida e é dividida em três partes: alerta, assistência e sabotagem. A engenharia social reversa envolve a criação de uma situação na qual o atacante necessita “ajudar” a vítima. Este é um bom caminho para se fortalecer a confiança, porque a vítima se sente obrigada a retribuir a ajuda. A engenharia social tem de colher as informações que estão facilmente disponíveis para não levantar suspeitas, por exemplo: telefones em uma lista, *e-mail* para contato, cadastros na internet, mídias sociais, etc.

Mitnick e Simon (2002) afirmam que o fator humano é o elo mais fraco na segurança da informação. Analisando a engenharia social por intermédio de casos hipotéticos apresentados por Mitnick e Simon é possível perceber que o engenheiro social explora vulnerabilidades na comunicação realizada nos relacionamentos sociais. É interessante pensar que qualquer ataque eficiente geralmente irá buscar o ponto fraco do sistema, assim como já verificado. A segurança de pessoas resume-se basicamente ao desenvolvimento e à execução de protocolos. Se não há sujeito a ser atacado, não há problema de segurança.

Todavia, existem aqueles que defendem que a engenharia social não é utilizada apenas para o mal. Atualmente, uma prática de mercado da segurança da informação é o teste de intrusão, uma espécie de teste de prevenção. O teste de intrusão simula ataques sucessivos com o objetivo de testar a segurança da informação e não comprometê-la a ponto de haver graves prejuízos. O propósito desse teste é conhecer os níveis de segurança da instituição e verificar a maturidade do ambiente de segurança. O processo é sistemático e de conhecimento da organização, as regras do teste são previamente

estabelecidas e os limites são acordados. O teste de intrusão é uma ferramenta de mercado para dar credibilidade, com o uso de um terceiro, à segurança da informação de uma organização (ALLEN, 2012). A engenharia social pode ser utilizada nos testes de intrusão.

A obra de Watson, Mason e Ackroyd (2014) apresenta uma metodologia completa de testes de intrusão utilizando a engenharia social, processo exposto na **Figura *24***. As etapas de sua metodologia cobrem todo o trabalho de teste de intrusão por meio da engenharia social, ensinando a modelar as ameaças; coletar informações sobre o alvo; criar um cenário de ataque para o alvo; executar o ataque para o cenário e editar o relatório de teste. Todo o processo metodológico é apoiado por ferramentas de ataque, técnicas de manipulação, estratégias de ataque, meios de ataque, formação de equipe. Portanto, pode-se pensar que a engenharia social não se constitui unicamente de ações maliciosas.

Um teste de intrusão utilizando engenharia social deve fazer no mínimo um reconhecimento do ambiente a ser atacado, construir um cenário de ataque, executar esse cenário e editar um relatório. A partir dessas etapas podem surgir outras, por exemplo, a criação de perfis falsos em mídias sociais, a elicitação – conversa estrategicamente elaborada, mas com aparência de informal, com o objetivo de colher informações –, ataques via *phishing* – *e-mails* fraudulentos –, infiltração na organização para colher informações (WATSON; MASON; ACKROYD, 2014).

Hadnagy (2011) crê firmemente que a engenharia social é uma ciência. O autor apresenta um *framework* para aplicação da engenharia social. O *framework* de Hadnagy inicia com a coleta de informações, elicitação do alvo, alegação para falsificação (pré-carga, do inglês *preload*), jogos mentais, técnicas de influenciar pessoas e integra tudo em seu *framework* com a utilização de ferramentas. Em seu *framework,* o ponto de seleção de um alvo é alcançado quando se junta possibilidade de falsificação, determinado grau de possibilidade de manipulação e acurado grau de ganância da vítima. Watson, Mason e Ackroyd (2014) afirmam que para um engenheiro social qualquer informação é útil em determinado momento.

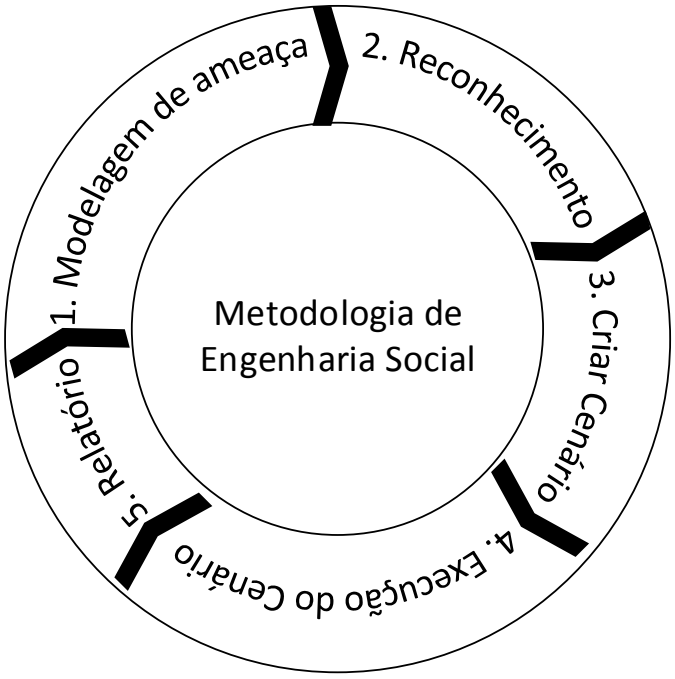


Figura 24. *Framework* de engenharia social

Fonte: WATSON; MASON; ACKROYD (2014; tradução do autor)

Hadnagy (2011) alega que o ser humano é um ser comunicante e precisa da comunicação para viver em sociedade. Em seu *framework* para engenharia social, a primeira etapa é a coleta de informações. Nesse momento ele informa que para seu *framework* nenhuma informação é irrelevante. A coleta de informações é uma etapa árdua e trabalhosa. Watson, Mason e Ackroyd (2014) afirmam que para um engenheiro social qualquer informação é útil em determinado momento.

Muitas vezes o indivíduo a ser explorado não possui um perfil (*profile*) bem definido na internet e não é fácil encontrar pegadas ou rastros de seu comportamento (*footprint*). A Agência Nacional de Segurança dos Estados Unidos define elicitação como a extração súbita de informação durante uma conversa normal e inocente. Para Hadnagy (2011), a etapa de elicitação serve para se descobrir algo por meio da lógica para ser efetivo nas próximas etapas do ataque. Na elicitação é necessário inovar nos questionamentos, e as palavras são utilizadas de tal forma que irão elevar as habilidades utilizadas nessa etapa.

Na atividade de elicitação, no *framework* de Hadnagy, temos a pré-carga (do inglês *preload*). A pré-carga é uma espécie de introdução ao golpe, podendo ser uma história para sensibilizar a vítima, imagens chocantes, etc. A ideia principal é tentar implantar ideias e

informações que induzirão uma reação da vítima. Algumas fragilidades que podem ser exploradas nessa fase são: o ego, o interesse mútuo, as falsas verdades, a apresentação de informação para obter outra. Portanto, uma boa elicitação é a criação de uma ponte para a próxima fase do ataque.

Para Watson, Mason e Ackroyd (2014), o *pretexting* é uma etapa do ataque na qual se cria um cenário para tentar convencer a vítima a fornecer determinadas informações. Para se criar um cenário perfeito, segundo os autores, é preciso inventar uma situação plausível, forjar um personagem detalhado. Nessa etapa pode-se enviar um presente ou agrado para conquistar a vítima, bem como utilizar pressão e autoridade. Para os autores, a engenharia social está muito ligada aos sentimentos dos envolvidos.

Segundo Hadnagy (2011), pré-carregar é a personificação, é a criação de um personagem, a produção de um cenário para tornar o indivíduo mais relaxado e livre de amarras para liberar as informações. A internet tem sido um ambiente muito propício para as personificações. O autor sugere para esta etapa uma pesquisa minuciosa para a construção do personagem, pois nesta fase o engenheiro social pode facilmente falhar, e ao menor passo em falso a vítima pode passar para o estado de desconfiança, e isso é exatamente o contrário do que o engenheiro social deseja.

A próxima fase do *framework* de Hadnagy são os jogos mentais e técnicas de influenciar pessoas. Nesta etapa, a observação e a aplicação de estímulos são muito utilizadas. Observar o comportamento da vítima, suas expressões corporais e verbais é parte dessa etapa. O indivíduo apresentou felicidade, raiva, espanto? Qual a reação para determinado estímulo? Ele tem algum vício? As táticas de influência incluem o uso dos sentimentos da vítima, como os de reciprocidade, obrigação, concessão, desgosto e autoridade. Atingir o indivíduo em seus sentimentos mais profundos para que ele se sinta obrigado a ajudar, a demonstrar reciprocidade por certa manifestação de sentimento, a ter compaixão e conceder algo, para enojá-lo e fazê-lo querer se ver livre de certa situação ou mesmo submetê-lo a uma falsa autoridade são consideradas táticas para influenciar as pessoas.

Hadnagy (2011) afirma que o problema das vítimas de golpes de engenharia social é que muitas delas estão cegas para os potenciais problemas devido à autoconfiança. O autor adverte que a engenharia social pura não é uma questão de bem ou mal, mas simplesmente uma ferramenta para diferentes situações e usos. Em diversas áreas e diversos momentos da vida a engenharia social é usada de forma não maliciosa.

Watson, Mason e Ackroyd (2014) trazem alguns casos emblemáticos de engenharia

social. Por exemplo, o ocorrido no escritório da RSA, escritório de segurança da informação da empresa EMC: em 2011 alguns *hackers* conseguiram quebrar a segurança da ferramenta *SecureID token*, muito usada em bancos em todo o mundo. Os maus elementos enviaram *e-mails phishing-scam* para funcionários do escritório que possuíam baixo privilégio no acesso a informações do local de trabalho. Ao persuadir as vítimas foi possível invadir a rede de computadores da empresa e escalar o privilégio de acesso, chegando ao objetivo de coletar informações para poder *hackear* o *SecureID token*. Esse ataque gerou prejuízos financeiros e para a imagem de organizações em todo o mundo, tornando-se um caso emblemático da composição de um ataque misto, utilizando engenharia social e outras técnicas de *hackers*.

Mitnick e Simon (2002) citam um exemplo de ataque com a utilização da ação de enganar, recurso da engenharia social. Nesse caso, o atacante manipula informações fazendo-se passar por funcionário de duas empresas contratadas pela empresa alvo. Ora o atacante utiliza informações de uma contratada para obter informações da segunda, ora se passa por representante da segunda contratada para obter informações privilegiadas da contratante. Com o intuito de aprofundar a análise, pode-se observar a seguir um caso completo de Mitnick e Simon (2002, p. 22).

> A senhora resolveu atacar um provedor de serviços de telefonia celular para saber se ela poderia localizar alguns engenheiros que estivessem tentados a atravessar a rua e ir trabalhar para um concorrente. Ela não podia ligar para a telefonista e dizer “quero falar com alguém que tenha cinco anos de experiência como engenheiro”. Em vez disso, por motivos que ficarão claros em alguns instantes, ela começou o assalto aos talentos buscando uma informação que parecia não ser nada sigilosa, uma informação que a empresa dá para quase todas as pessoas que a pedem.
>
> **A primeira ligação: a recepcionista**
>
> Usando o nome Didi Sands, a atacante fez uma ligação para os escritórios da empresa de telefonia celular. Esta foi parte da conversação:
>
> Recepcionista: Boa tarde. Sou Marie. Posso ajudar?
>
> Didi: Você pode me passar para o Departamento de Transportes?
>
> R.: Eu não sei se temos um, vou procurar na minha listagem. Com quem falo?
>
> D.: Aqui é Didi.
>
> R.: Você está ligando do prédio ou...?

D.: Não, eu estou fora do prédio.

R.: Didi de quê?

D.: Didi Sands. Eu tinha o ramal de Transportes, mas esqueci.

R.: Um momento.

Para evitar suspeitas, nesse ponto Didi fez uma pergunta casual só para manter a conversação, com a intenção de estabelecer o fato de que ela estava “por dentro” e familiarizada com as localizações da empresa.

D.: Em qual prédio você está – Lakeview ou Main Place?

R.: Main Place (pausa). O número é 805 555 6469.

Para ter um *backup* caso a ligação para Transportes não fornecesse aquilo que ela estava procurando, Didi disse que ela também queria falar com Imóveis. A recepcionista deu esse número também. Quando Didi pediu para ser transferida para Transportes, a recepcionista tentou, mas a linha estava ocupada.

Nesse ponto, Didi pediu um *terceiro* número de telefone, o de Contas a Receber, o qual estava localizado em um prédio corporativo em Austin, no Texas. A recepcionista pediu para ela aguardar um momento e saiu da linha. Ela estava consultando a Segurança dizendo que estava com uma ligação telefônica suspeita e achou que havia algo de estranho.

De forma alguma, responderam, e Didi não teve a menor preocupação. Ela estava ficando meio aborrecida, mas para a recepcionista isso tudo fazia parte de um dia normal de trabalho. Após cerca de um minuto, a recepcionista voltou à linha procurou o número de Contas a Receber, fez a transferência e colocou Didi na linha.

A segunda ligação: Peggy

A próxima conversação foi assim:

Peggy: Contas a Receber, Peggy.

Didi: Oi, Peggy. Aqui é Didi, de Thousand Oaks.

P.: Oi, Didi.

D.: Como vai?

P.: Tudo bem.

Em seguida, Didi usou um termo familiar no mundo corporativo que descreve o código de cobrança para designar as despesas no orçamento de uma organização ou grupo de trabalho específico:

D.: Excelente. Tenho uma pergunta. Como encontro o centro de custo de determinado departamento?

P.: Você tem de falar com o analista de orçamento do departamento.

D.: Você sabe quem é o analista de orçamento para Thousand Oaks – a sede? Eu estou tentando preencher um formulário e não sei qual é o centro de custo apropriado.

P.: Só sei que quando você precisa do número do centro de custo, você liga para o seu analista de orçamento.

D.: Você tem um centro de custo no seu departamento aí no Texas?

P.: Temos o nosso próprio centro de custo, mas eles não nos dão a lista com todos eles.

D.: Quantos dígitos têm o centro de custo? Por exemplo, qual é o seu centro de custo?

P.: Bem, você trabalha no 9WC ou no SAT?

Didi não tinha a menor ideia de quais eram esses departamentos ou grupos, mas isso não importava. Ela respondeu:

D.: 9WC.

P.: Então em geral são quatro dígitos. Onde você disse que trabalhava?

D.: Na sede, em Thousand Oaks.

P.: Bem, aqui tem um para Thousand Oaks, Ê 1A5N, com N de Nancy.

Falando apenas o tempo suficiente com alguém que estava disposto a ajudar, Didi conseguiu o número do centro de custo de que precisava – uma daquelas informações que ninguém pensa em proteger, porque parece algo que nunca terá valor para uma pessoa de fora.

A terceira ligação: um número errado útil

A próxima etapa para Didi seria explorar o número do centro de custo e transformá-lo em algo de valor verdadeiro, usando-o como uma ficha de pôquer.

Ela começou ligando para o departamento de Imóveis fingindo ter ligado para um número errado. Começando com um “desculpe incomodar, mas…”, ela disse que era uma funcionária que havia perdido a lista de telefones da empresa e perguntou para quem ela deveria ligar para conseguir outra cópia. O homem disse que a cópia impressa estava desatualizada, porque ela estava disponível no *site* da intranet da empresa.

Didi disse que preferia usar uma cópia impressa, e o homem disse para ela ligar para Publicações e, em seguida, sem que ela pedisse – talvez só para manter a senhora com voz *sexy* mais um pouco na linha – procurou o número e o forneceu para ela.

A quarta ligação: Bart, em Publicações

Em Publicações, ela falou com um homem chamado Bart. Didi disse que era de Thousand Oaks e que eles tinham um consultor novo que precisava de uma cópia da lista de telefones da empresa. Ela disse que uma cópia impressa funcionaria melhor para o consultor, mesmo que estivesse meio desatualizada. Bart disse que ela teria de preencher um formulário de requisição e enviá-lo para ele.

Didi disse que estava sem formulários e com muita pressa e perguntou se Bart não poderia fazer o favor de preencher o formulário para ela. Ele concordou, não muito entusiasmado, e Didi forneceu os detalhes. Com o endereço da contratada fictícia, ela deu o número daquilo que os engenheiros sociais chamam de *rnail drop,* o qual, nesse caso, era uma empresa de caixas postais na qual a sua empresa alugava caixas postais para situações como aquela.

A preliminar anterior tornou-se útil agora: seria cobrada uma taxa pelo custo e pelo envio da lista. Muito bem – Didi deu o centro de custo de Thousand Oaks:

"1A5N, com N de Nancy".

Alguns dias depois, quando chegou a lista de telefones corporativos, Didi descobriu que isso valia mais a pena do que ela havia imaginado: ela não apenas tinha os nomes e os números de telefones, mas também quem trabalhava para quem – a estrutura corporativa de toda a organização.

A senhora de voz forte estava pronta para começar a caçar seu talento e fazer ligações telefônicas em busca de pessoas. Ela havia trapaceado as informações que precisava ter para iniciar seu ataque usando o dom da palavra lapidado ao

> máximo que cada engenheiro social habilidoso tem. Agora ela estava pronta para receber a recompensa.
>
> […]
>
> Assim como as peças de um quebra-cabeça, cada informação parece irrelevante sozinha. Porém, quando as peças são juntadas, uma figura aparece. Neste caso, a figura do engenheiro social mostrou toda a estrutura interna da empresa.

Pode-se facilmente transportar o exemplo anterior para a realidade de uma organização da administração pública, onde são firmados centenas de contratos por ano com diferentes contratadas e com controles dispersos. Em determinadas situações não há controles de segurança da informação bem definidos entre as partes. Esse cenário proporciona a cada indivíduo um papel que poderia ser o caso do golpe apresentado. Muito se faz para que a contratação dê certo, sendo os fins da contratação o objetivo principal. Mas possivelmente não há controle das comunicações observando esse nível de ataque. Em uma situação clara de manifestação de conflitos de interesse e troca de recursos escassos há risco de trapaças, porque, como diz Schneier (1998), o elo mais fraco em qualquer sistema de segurança é o pobre ser humano tentando ver seu trabalho feito e querendo ajudar outros se puder.

Watson, Mason e Ackroyd (2014) garantem que se um funcionário é treinado para ser totalmente prestativo ele não medirá esforços para solucionar os problemas que aparecerem. Por sua vez, o engenheiro social irá se utilizar dessa prestatividade para apresentar um problema a esse funcionário, e este provavelmente tentará de tudo para resolvê-lo. Obviamente quando o funcionário solucionar o problema terá ajudado o engenheiro social no seu propósito.

Watson, Mason e Ackroyd (2014) apresentaram o caso ocorrido no Palácio de Buckingham, quando um invasor entrou no palácio por meio de uma vaga em um cargo de manutenção. O invasor ficou lotado no palácio por semanas, entrando em salas e tirando fotos do local. Foi um escândalo que abalou a “estrutura” da segurança do palácio. O engenheiro social busca conhecer os processos internos, o dialeto, o jargão da organização e os utiliza como arma para se infiltrar ou construir cenários que possam prover-lhe alguma vantagem (DOLAN, 2004).

Outro caso interessante apresentado por Watson, Mason e Ackroyd (2014) foi a coleta de dados pessoais dos clientes do videogame XBOX, da Microsoft. Nesse caso, as contas de usuário foram copiadas e utilizadas em engenharia social. Foram coletadas

informações de funcionários na internet que estavam espalhadas, aparentemente publicadas sem propósito de exposição. As informações foram coletadas e unidas como um quebra-cabeça e exploradas. Para Turner (2005), um engenheiro social muito competente pode ter a meta de obter a confiança de tal forma que a vítima fornece casualmente informação interna sensível. O autor afirma que muitas vezes pode não se tratar de uma divulgação de informação significativa em si, mas a informação pode ser combinada com outros pequenos pedaços de informação para produzir um roteiro detalhado e perigoso, gerando informações ricas sobre o alvo.

Gragg (2002) define uma defesa multinível que aborda os gatilhos psicológicos, sendo os níveis de defesa definidos em política de segurança, treinamento de conscientização de segurança, treinamento de resistência, lembretes, minas terrestres para engenharia social (Selm) e de resposta a incidentes. Selm são procedimentos ou políticas que, quando implementados, agem como um sistema de detecção de intrusão da engenharia social, ou seja, geram alertas a partir de comportamentos preestabelecidos dos usuários, por exemplo, um acesso a um arquivo ou caixa de *e-mail.*

Segundo Dolan (2004), para poder se defender de ataques de engenharia social é preciso criar rotinas de treinamento que contemplem esclarecimentos sobre comportamento seguro diante das principais técnicas de engenharia social e uma sólida política de segurança. Essas estratégias devem conter as diretivas de senha, as avaliações de vulnerabilidade, a classificação de dados, a política de controle de acesso, testes de penetração, o processo de concessão e rescisão de privilégios, resposta a incidentes, segurança física e conscientização de segurança.

Turner (2005) julga que as organizações podem ajudar a garantir a segurança realizando programas e cursos de conscientização. Para ele, as intranets organizacionais podem ser um recurso valioso para essa abordagem, especialmente boletins *on-line*; lembretes por *e-mail*, jogos focados em treinamento e rigorosos requisitos de mudança de senha estão incluídos. O autor esclarece que o maior risco seria os funcionários se tornarem complacentes e se esquecerem da importância da segurança. Por isso, a aplicação de um processo contínuo de conscientização em toda a organização é a chave para a proteção permanente e a criação de uma cultura consciente de segurança na organização. Turner recomenda, inclusive, a realização de testes no ambiente organizacional contra os ataques de engenharia social.

Rybczynski (2000) acredita que a conscientização do usuário é a chave para manter a integridade dos sistemas de informação. Logo, é preciso informar o pobre ser humano,

por meio da conscientização e do, que nem sempre o caminho mais curto para o seu trabalho ser feito é o melhor caminho para a organização. Como um dos principais pontos de vulnerabilidade dos sistemas de segurança são as pessoas, a educação é um fator importante.

Gragg (2002) explica que a engenharia social é o processo de enganar as pessoas e lhes retirar informações confidenciais ou privilegiadas. O autor afirma que enquanto houver abundância de informações para se realizar a engenharia social essa ameaça será considerada muito real e não facilmente defendida.

Para Hadnagy (2011), o engenheiro social preocupa-se com o fluxo das informações nas comunicações, construindo pontes entre espaços onde normalmente existem falhas de relacionamento. Hadnagy define comunicação como o processo de se transmitir informações de um ente a outro, presumindo-se a interação entre pelo menos duas pessoas. O engenheiro social constrói confiança e um objetivo comum para poder chegar ao seu real objetivo por meio da comunicação.

Segundo Hadnagy (2011), o engenheiro social precisa conhecer os modelos de comunicação, de Shannon e Weaver até os modelos mais contemporâneos, pois estes serão muito úteis na construção da estratégia de ataque. Quando o engenheiro social constrói a estratégia de comunicação ele precisa trabalhar com os modelos de comunicação de forma reversa. Não montar um bom plano e não ter um modelo de comunicação irá provavelmente levar o ataque ao fracasso.

Portanto, o que pode ser concluído é que a engenharia social é um problema sério, real e geralmente a porta de entrada para a aplicação de outras formas de ataque em SIC. A empresa deve não só estabelecer uma boa política de segurança da informação para se proteger, mas também ter um programa eficaz de conscientização e treinamento de segurança. O programa de conscientização/capacitação não deve apenas reiterar as políticas de segurança, deve educar os usuários quanto aos métodos utilizados pelos engenheiros sociais e os riscos envolvidos.

3.4.1 Ferramentas de engenharia social

Apesar de a engenharia social ter como objetivo um ataque que envolve, em essência, o fator humano, existem tecnologias que podem ser usadas para potencializar

os ataques. Algumas dessas ferramentas são o Dradis,[12] Barket,[13] Maltego,[14] Toolkit SET (Social Engineer Toolkit).

No esforço de se montar um perfil podem-se utilizar as ferramentas Dradis e Barket. Com essas duas ferramentas é possível construir um perfil da vítima no formato de estruturas hierárquicas, facilitando a visualização. Podem ser incluídos nessas ferramentas os resultados de buscas em *sites* como Whois, nas mídias sociais, no Google Maps e no Earth (HADNAGY, 2011).

Destaque-se aqui o Toolkit SET (Social Engineer Toolkit), um poderoso conjunto de ferramentas, um verdadeiro “canivete suíço” da engenharia social. Basicamente o SET é um conjunto de *scripts python*[15] *e metasploit*.[16] Com o SET há diversas possibilidades de ataque.

O SET é projetado especificamente para executar ataques variados contra o elemento humano. Os ataques incorporados ao conjunto de ferramentas do SET são projetados para serem focados em uma pessoa ou em uma organização. Esse “canivete suiço” de ataques de engenharia social está sendo muito utilizado durante os testes de penetração, ou testes de intrusão (WATSON; MASON; ACKROYD, 2014).

O SET é um conjunto de ferramentas baseado em interface puramente textual. O conjunto de ferramentas é acessado por um menu. Na Figura 25 pode-se ver o menu principal do conjunto de ferramentas. Com essa ferramenta podem ser feitos vários ataques diferentes, um deles é o envio de *e-mails* em massa, quando um *e-mail* falso é enviado para instalar um aplicativo ou realizar um *phishing-scan*, coletando informações específicas (WATSON; MASON; ACKROYD, 2014). No menu principal, pode-se observar a variedade de ataques que esse poderoso conjunto de Toolkit possui, selecionando a opção 1, tem-se o seguinte:

1) Spear-Phishing Attack Vectors;
2) Website Attack Vectors;

---

[12] Dradis é um *framework* ou uma plataforma de relatórios para os especialistas em segurança de TI. Disponível em: <http://dradisframework.org/>.
[13] Barket é um aplicativo de anotações multiúso. Disponível em: <http://basket.kde.org/>.
[14] Maltego é uma ferramenta para atividades de inteligência e investigação forense. Ele oferece facilidades para a mineração de dados e a representação de informações. Com o uso do Maltego há a possibilidade de se reunir informação organizando e catalogando. Disponível em: <https://www.paterva.com/web6/>.
[15] O Python é uma linguagem interpretada de programação– aquela linguagem que não necessita de compilação – em *script* – arquivos de texto, geralmente escritos em linguagem *english like. Maiores informações favor verificar em http://www.python.org.*
[16] O Metasploit é uma ferramenta utilizada em testes de intrusão, disponível em http://www.rapid7.com/products/metasploit/

3) Infectious Media Generator;
4) Create a Payload and Listener;
5) Mass Mailer Attack;
6) Arduino-Based Attack Vector;
7) SMS Spoofing Attack Vector;
8) Wireless Access Point Attack Vector;
9) QRCode Generator Attack Vector;
10) Powershell Attack Vectors;
11) Third Party Modules;
99) Return back to the main menu.

Shostack e Stewart (2008) definem o *phishing* como o envio de *e-mails* fraudulentos mas que parecem amigáveis. Segundo os autores, a meta dos *phishers* é atrair alguma ação da vítima. Eles apresentam o caso no qual as autoridades turcas efetuaram a prisão de Ali Y'nin e de mais nove cúmplices por fraude a bancos. A gangue enviou por volta de 11 mil *e-mails* infectando computadores por vírus. Os usuários, persuadidos pelos *e-mails*, instalaram um *software* que monitorava seu comportamento e colhia seus dados bancários.

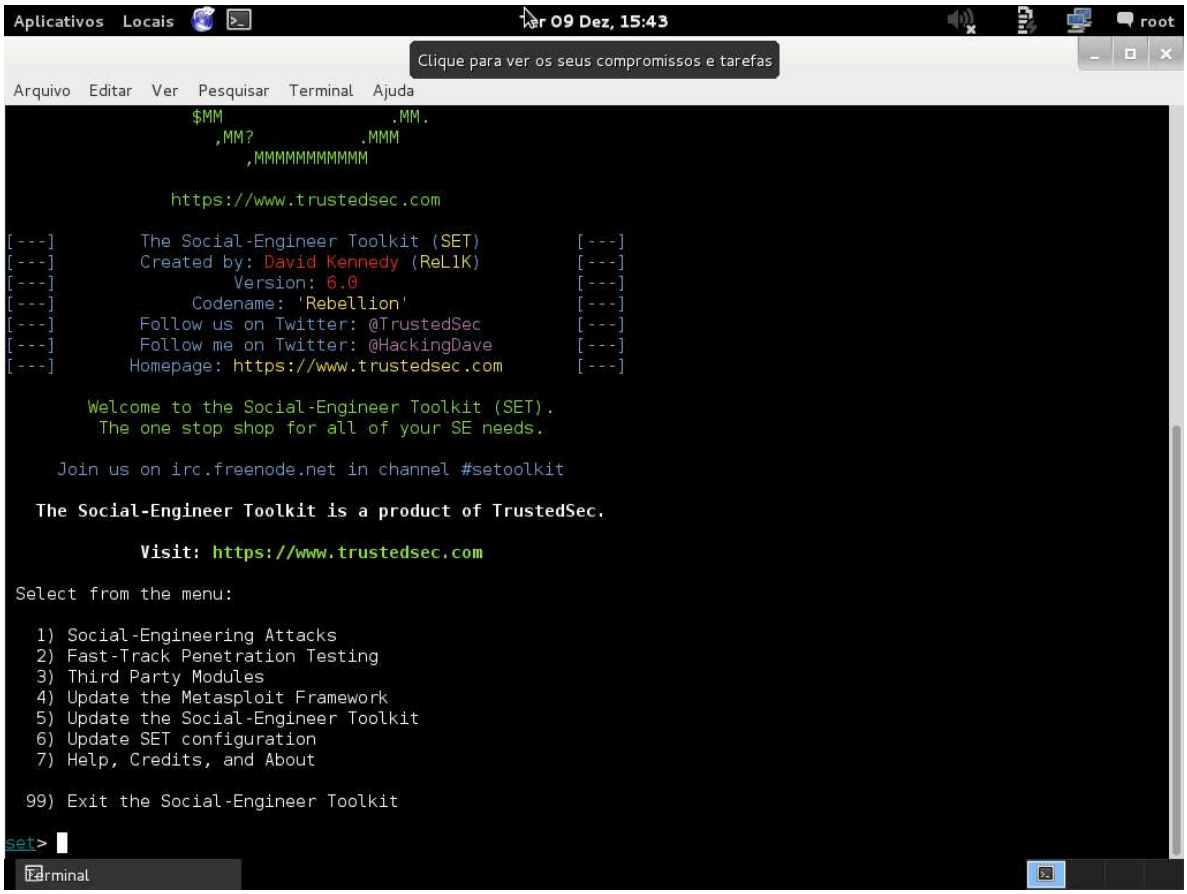


Figura 25. Menu principal do ToolKit SET (Social Engeneer Toolkit)

O SET possui a ferramenta *set-automate*, e com ela é possível automatizar os ataques. Utilizando-se o comando *set-automate arquivo.txt* é factível extrair do arquivo os comandos de navegação do menu e as entradas para as ferramentas de ataque *metasploit*. A seguir tem-se um exemplo que enviará um *e-mail* automaticamente. Esse processo pode ser repetido indefinidamente e estará em um arquivo texto automatizando os passos do ataque.

1
5
1
vitima@provedor.com
1
seuemail@provedor.com
FROM : Presidente
email_password
BODY: teste teste teste teste END

Outra ferramenta interessante é o *thehasvest*. Essa ferramenta executa busca por endereços de *e-mail*. Ela encontra endereços de *e-mail* a partir do domínio do provedor de *e-mail*, encontra subdomínios e seus *e-mails* presentes na web. Esta é uma ferramenta de linha de comando e pode ser parametrizada para realizar diferentes tipos de busca. O comando theharvest –d provedor –b google utilizará o engenho de busca do Google para encontrar todos os *e-mails* para o determinado provedor publicados em seu domínio (WATSON; MASON; ACKROYD, 2014).

Portanto, embora a engenharia social seja um ataque que envolve, em essência, pessoas, existem tecnologias que potencializam os ataques. Das ferramentas apresentadas, o SET é considerado a mais poderosa. Com o SET seria factível um ataque via e-*mail* automatizado, e isso potencializaria a seleção de alvos, pois seria possível verificar por outro meio as vulnerabilidades.

3.5 Fundamentos da análise de redes sociais

Há quem defenda que as relações humanas e sociais são pautadas pela incerteza e que geralmente sua análise é baseada em intuição. Os métodos de análise de redes sociais são úteis quando se está interessado em investigar o comportamento social baseado na estrutura em rede. Nesta seção serão definidos a análise de redes sociais (ARS) e alguns conceitos inerentes à disciplina com o intuito de entender como estudar a confiança, consequentemente a engenharia social, utilizando esta metodologia de análise. A intenção desta seção não é esgotar o assunto, que é muito amplo, mas apenas apresentar uma base para continuar este estudo.

3.5.1 Análise de redes sociais (ARS)

Para Wasserman e Faust (1994), a análise de redes sociais trata de processos de desenvolvimento de modelos, especialização e medição. Assim, por meio de definições formais, medição e análise pode-se entender a estrutura da rede e encontrar padrões. Segundo os autores, existe um vocabulário próprio para essa área do conhecimento que auxilia na discussão de conceitos e na apresentação de ideias.

Consoante Everton (2013), a análise de redes sociais é uma coleção de teorias e métodos que assumem que o comportamento de um ator (podendo ser um indivíduo, grupos ou organizações) é profundamente afetado pelas relações com os outros e pelas modificações da rede como um todo. Mais do que observar como os atores são afetados pelo que está ao seu redor, a ARS admite que somos seres sociais e temos padrões de interação que afetam o que fazemos e o que acreditamos. O objetivo primário da ARS é desenvolver métricas que ajudem os analistas a obter um melhor entendimento das particularidades da estrutura de uma rede.

Wasserman e Faust (1994) afirmam que as ciências sociais geralmente ignoram “padrões” sobre as informações relacionais. Sacerdote e Fernandes (2013, p. 131) definem a ARS como

> [...] uma metodologia de análise de dados relacionais que permite o estudo de fenômenos sociais. [...] a ARS possibilita encontrar tendências ou padrões de comportamento, pois o seu foco é o conjunto das relações que os atores sociais estabelecem entre si, influenciando o desempenho de propriedades e funções dessa rede de relações.

Marteleto e Tomaél (2006) argumentam que as redes sociais se relacionam a um conjunto de pessoas (ou organizações ou outras entidades sociais) conectadas por

relacionamentos sociais determinados pela amizade, pelo trabalho ou pela troca de informações, e por meio dessas ligações são construídas e reconstruídas as estruturas sociais.

Marteleto e Tomaél (2006) afirmam ainda que as redes sociais expressam o mundo em movimento. Turner (1991) defende que a fundamentação de conceitos em matemática para as redes sociais pode oferecer maior precisão e fornecer uma linguagem comum para reunir um núcleo conceitual comum às várias disciplinas que se sobrepõem quando utilizam aspectos mais flexíveis da sociologia.

Segundo Silva e Ferreira (2005), a ARS interessa a pesquisadores de vários campos do conhecimento. Estes, na tentativa de compreenderem seu impacto sobre a vida social, deram origem a diversas metodologias de análise que têm como base as relações entre os indivíduos, numa estrutura em forma de redes. De acordo com os autores, embora exista uma discussão epistemológica em torno da posição da ARS nas Ciências Sociais, observa-se que a fundamentação matemática facilita o desenvolvimento de uma linguagem comum que aproxima pesquisadores de várias áreas, com métodos de coleta e análise de dados que podem ser utilizados em vários modelos teóricos.

Portanto, na sociometria[17] entende-se que a sociedade é representada por uma estrutura formada por atores e suas relações. Um sociograma é uma figura, um recorte, no qual as pessoas (ou, mais genericamente, qualquer ente social) são representadas por vértices, ou pontos, num espaço dimensional, e as relações entre os pares de vértices, ou atores, são representadas por linhas. Alguns autores utilizam matrizes eficientemente para representar redes sociais. Com a utilização de matrizes é possível se valer da álgebra e da Teoria dos Grafos nas redes sociais. A partir disso, os modelos matemáticos, sejam estocásticos sejam determinísticos, estarão disponíveis para a aplicação e os estudos de análise de redes sociais.

Gersting (1995) define grafo como um conjunto não vazio de nós (vértices) e um conjunto de arcos (arestas) tais que cada arco conecta dois nós. Segundo De Nooy, Mrvar e Batagelj (2011), o grafo é um conjunto de vértices e um conjunto de linhas que liga pares de vértices. O vértice é a menor unidade de uma rede, sua unidade atômica. Na ARS o vértice representa os atores (pessoas, organizações, etc.), e as linhas são relações entre os vértices. Na ARS a linha representa as relações entre os atores sociais. O *loop* é um tipo

[17] J. L. Moreno fundou a ciência social chamada sociometria, a qual estuda as relações interpessoais. A análise de redes sociais é fundamentada em informações relacionais e estruturais (WASSERMAN; FAUST, 1994).

especial de linha, é a linha que conecta o vértice a ele mesmo. A linha pode ser dirigida e não dirigida. A linha dirigida é a que leva em consideração o sentido e é chamada de arco. A linha não dirigida é chamada de borda. Os grafos dirigidos (**Figura *26***), ou dígrafos, contêm um ou mais arcos – linhas com direção definida. Os grafos não dirigidos (**Figura *27***) são os que possuem apenas bordas.

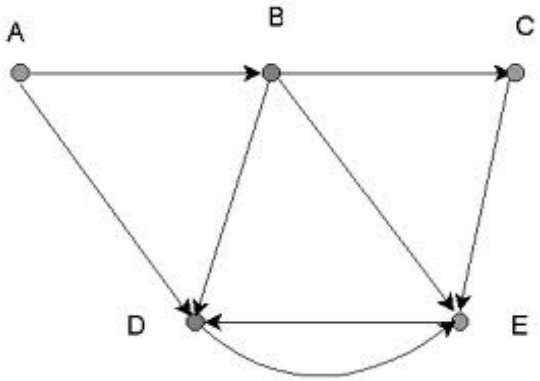


Figura 26. Grafo dirigido

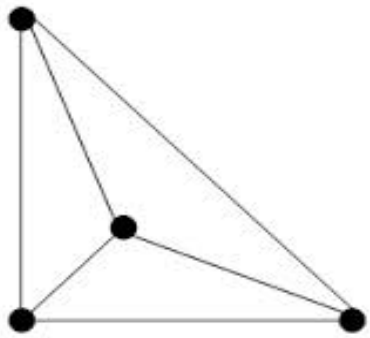


Figura 27. Grafo não dirigido

A ARS utiliza técnicas que promovem precisão e definição formal para os estudos sociais. Os modelos de redes sociais, sociogramas, podem ser avaliados por meio de termos e conceitos ou processos relacionais, que geralmente podem ser representados matematicamente (WASSERMAN; FAUST, 1994). Turner (1991) informa que a análise de redes é uma disciplina interdisciplinar, e as unidades inseridas na rede podem ser pessoas, organizações, atores corporativos e outras entidades, com aspectos das ciências exatas sendo amplamente utilizados. Para o autor, existem pontos, atores, que precisam ser conectados de alguma maneira para formar as estruturas sociais. Essas conexões foram vistas originalmente como *links*, mas foram alteradas para linhas. Do ponto de vista matemático, linhas são apenas linhas, mas do ponto de vista sociológico as linhas têm significado – são as relações entre os nós da rede.

Everton (2013) explica que na ARS o termo ator se refere discretamente a indivíduos, subgrupos, organizações, coletividades, comunidades, nações e a tudo mais que pode ser envolvido em relações sociais. Conforme o autor, atores são ligados por linhas, e as linhas podem variar em tipo, força e direção. Ele defende que as linhas na ARS podem ter a função de condutores da difusão de vários tipos de benesses materiais e não materiais na rede social, tais como informações, sentimentos, recursos, normas, doenças, opiniões e

confiança.

Na análise de redes sociais os atores da rede social e suas ações são vistos como interdependentes, ou seja, a rede é vista como um elemento autônomo. Uma ação de um ator pode refletir na ação dos demais atores de uma rede. As relações entre os atores, representadas no sociograma como linhas, são canais para a interação e para a transferência ou o fluxo de recursos (materiais e não materiais) entre os atores (WASSERMAN; FAUST, 1994). A seguir, apresenta-se, na Figura 28, um exemplo de sociograma, rede social, retirado de De Nooy, Mrvar e Batagelj (2011).

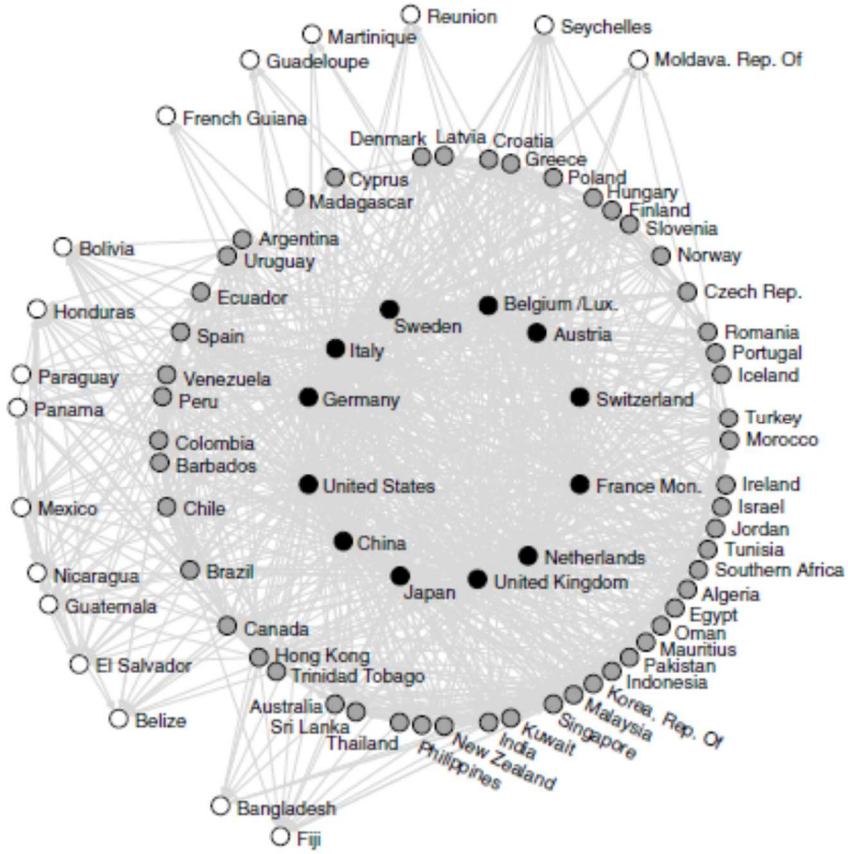


Figura 28. Mercado de manufatura de metais e partições (*clusters*)

Fonte: DE NOOY; MRVAR; BATAGELJ (2011)

A **Figura *28*** representa a rede social do mercado de manufatura de metais e uma classificação mundial dos países em um estudo realizado em 1994. Russell (2013) doutrina que o *clustering* envolve criar coleções de itens e particioná-los em pequenos grupos de acordo com uma heurística, usualmente desenhada comparando-se os elementos da coleção. Para De Nooy, Mrvar e Batagelj (2011), uma partição seria uma classificação ou um agrupamento de vértices em uma rede tal que cada vértice pertença a exatamente uma classe ou agrupamento. No sociograma da **Figura *28*** existem três partições: vértices pretos,

cinzas e brancos.

O grau de um nó é o número de linhas que incidem sobre ele, podendo este ser dividido em grau de entrada e grau de saída. O grau de entrada são os arcos que o vértice recebe, e o grau de saída são os arcos que o vértice envia, respectivamente.

Para De Nooy, Mrvar e Batagelj (2011), o objetivo principal da análise de redes sociais é a detecção de padrões no sociograma. Uma rede consiste em um grafo e em informações adicionais nos vértices e nas linhas. Turner (1991) reforça que é importante mencionar que as direções das linhas representam o sentido no qual os recursos fluem na rede. As setas são colocadas nos dígrafos para indicar a direção daquela linha.

Everton (2013) define caminho (*path*) na rede social por meio do caminhar (*walk*) – que é uma sequência de atores e linhas –, sendo o caminho um caminhar sem repetição de atores entre o primeiro e o último vértice. Everton informa que a distância entre dois nós é o número de saltos em um caminho sem repetição. Além disso, o autor traz o conceito de topografia de uma rede social, sendo ela a estrutura geral da rede. Isso não pode ser confundido com o *layout,* que é a forma visual da rede em um instante. O *layout* de uma rede pode mudar no tempo, mas a topografia da rede não. Caso a rede seja transformada, a topografia da rede terá sido alterada, e assim ter-se-á uma nova rede.

Uma rede é diferente da outra em termos de topografia. Everton (2013) evidencia que o comportamento dos atores sofre forte influência e impacto provenientes da topografia da rede. Ele informa sobre o conceito de densidade, métrica de interconectividade de uma rede: quanto mais densa uma rede, mais interconectada ela é, podendo chegar à densidade 1, quando a rede é totalmente interconectada, ou seja, todos os atores se ligam a todos os outros. Para o autor, é mais provável um ator seguir normas e sofrer influência quando está em uma rede densa.

Aqui se pode refletir sobre o fenômeno da homofilia – “pássaros iguais tendem a voar juntos”. Everton (2013) afirma que os atores de uma rede interagem com aqueles que consideram semelhantes, e as interações repetitivas podem levar a emergir formações sociais como micro (individuais), meso (grupos) e macro (instituições, nações). De Nooy, Mrvar e Batagelj (2011) afirmam que é esperado que pessoas similares, que se identificam, interajam mais, pelo menos mais frequentemente que pessoas que não se identificam, não similares. É esperado que os membros de um mesmo grupo interajam mais, possivelmente porque existe mais confiança entre seus elementos. Deve-se lembrar da influência dos círculos de distância emocional no estabelecimento da confiança.

Para De Nooy, Mrvar e Batagelj (2011), na ARS a difusão é um caso especial de

brokerage, denominado corretagem com uma dimensão temporal (redes longitudinais). Algo – doença, produto, opinião ou atitude – é entregue por uma pessoa a outra no curso do tempo. Os autores assumem que as relações sociais são instrumentos do processo de difusão. Essas relações são o canal de persuasão e contágio social. Logo, os autores definem *brokerage* como a corretagem no tempo, a mediação social, podendo ser uma métrica de capital social. Assim, se uma empresa é considerada confiável e esse hábito de confiar nela é passado de tempos em tempos, seu capital social é considerado alto.

Conforme De Nooy, Mrvar e Batagelj (2011), a métrica de centralidade é baseada nas interconexões entre os atores da rede – quanto mais interconectado é um nó, mais central ele está na rede, então mais nuclear ele é. Voltando à **Figura *28***, pode-se observar que os países pertencentes ao *cluster* preto possuem maior centralidade que os países pertencentes aos agrupamentos cinza e branco. A centralidade pode ser medida de diversas formas, por exemplo, pelo grau do nó, pela distância relativa daquele nó em relação aos demais atores da rede.

Everton (2013) ensina que a intensa interação social permite a criação de um sentimento de grupo e solidariedade, normas de comportamento e símbolos de pertencimento ao grupo (bandeiras, tatuagens de gang, cruz cristã) e um senso de identidade. Uma pessoa que possui muitos amigos tem mais chance de conseguir ajuda ou informação porque tem maior capital social. O grau do nó pode ser uma medida de capital social, ele pode ser usado para se conseguir vantagens. Mas os analistas de redes sociais descobriram que não é apenas o grau que determina o capital social, os tipos de linhas também são importantes. Ter muitas conexões com pessoas de um mesmo grupo expõe o ator às mesmas informações que circulam no grupo. Mas quem se conecta com vários grupos tem maior entrada e acesso informacional variado (DE NOOY; MRVAR; BATAGELJ, 2011).

Dois vértices são adjacentes se são conectados por pelo menos uma linha, podendo também ser chamados de vizinhos. Por sua vez, o conjunto de todos os vizinhos de um nó da rede é sua rede ego. Muitos métodos de análise de redes sociais são focados nas relações diádicas e triádicas das redes ego dos vértices. As relações diádicas são a composição da linha que liga dois atores de uma rede e os vértices que os representam. As relações triádicas são a composição das linhas e os três vértices de uma estrutura, três atores de uma rede social e seus relacionamentos (WASSERMAN; FAUST, 1994).

Segundo De Nooy, Mrvar e Batagelj (2011), um grafo sinalizado é aquele que possui em seus vértices sinais positivos e negativos. Um ciclo é um elemento estrutural fechado

no qual sempre haverá um caminho entre os vértices. Na **Figura *29*** encontra-se um grafo sinalizado e cíclico que possui duas pessoas e uma coisa. Observe-se que P tem uma relação positiva com a coisa X e que a outra pessoa O não tem.

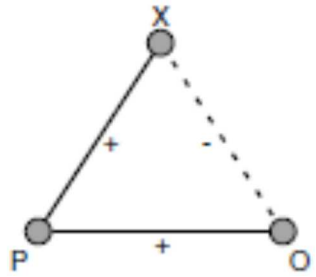


Figura 29. Uma pessoa, outro e X (coisa)

Fonte: DE NOOY; MRVAR; BATAGELJ (2011)

Para De Nooy, Mrvar e Batagelj (2011), um grafo sinalizado está balanceado se ele pode ser particionado em dois agrupamentos (*clusters)* de forma que todas as linhas positivas estejam dentro de um *cluster* e todas as linhas negativas estejam ligando esses *clusters*. Por exemplo: suponhamos três grupos coesos que possuem relações positivas entre os elementos de seu grupo. Nessa suposição esses atores sociais possuem relações negativas entre os demais atores dos outros grupos.

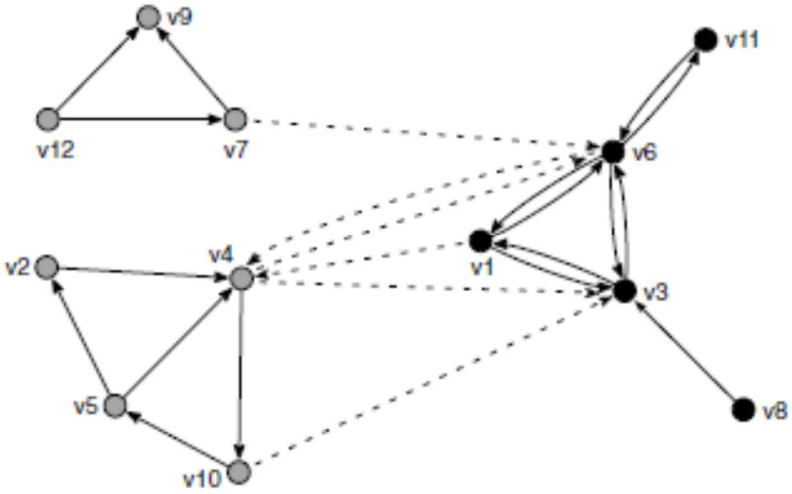


Figura 30. Grafo balanceado

Fonte: DE NOOY; MRVAR; BATAGELJ (2011)

Everton (2013) especifica que os analistas geralmente analisam os dados de uma rede social sob uma ou duas óticas: (1) relacional ou (2) abordagem posicional. Todas as métricas apresentadas até o momento nesta tese tratam da abordagem relacional. A abordagem posicional é mais focada na posição do ator na estrutura, não observa a totalidade da rede, procura a identidade estrutural, nota a equivalência de estruturas. Essa abordagem não exclui a importância das métricas de densidade, como, por exemplo, a centralidade.

As posições de ponte (*bridge)* e corretagem (*broker*) são muito importantes para este estudo. Os pontos de lacunas na rede são preenchidos por essas posições. Por exemplo: na **Figura *30***, a linha que liga V_7 à V_6 é uma *bridge* – e V_7 seria o corretor do ator V_9 diante dos recursos provenientes do *cluster* preto. V_{12} não tem relacionamento suficiente para receber recursos de seu *cluster*, como pode ser visto, ele só possui relacionamento direcional com saída.

Um buraco estrutural é uma relação diádica ou triádica que torna um dos elementos da relação um mediador. O fenômeno das *bridges* é o principal responsável pelo surgimento dos buracos estruturais. Por meio dessas lacunas de linhas de condução dos recursos certos atores tornam-se mais fortes e podem vir a ser corretores dos demais no fluxo desses recursos (EVERTON, 2013).

O fenômeno da representação social, ou mediação, em alguns casos ocorre por decisão do grupo. Por meio do capital social de um ator o grupo o seleciona para mediar situações ou para representá-lo. Os casos de mediação social devem-se à posição do ator na rede. Observem-se as tríades u, v e w da **Figura *31***. Verificam-se cinco papéis sociais de corretagem, mediação e representação, onde v será sempre o mediador. Na figura pode-se ver que os buracos estruturais geram oportunidades de mediação para determinados atores (DE NOOY; MRVAR; BATAGELJ, 2011).

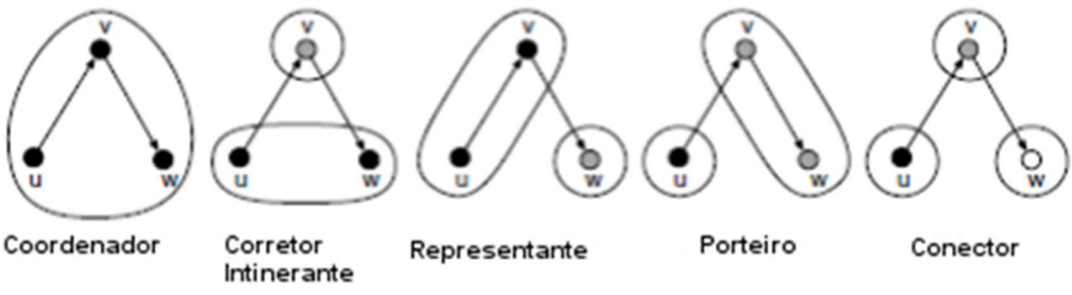


Figura 31. Papéis de corretagem em uma rede social

Fonte: DE NOOY; MRVAR; BATAGELJ (2011)

No primeiro papel da **Figura *31*** tem-se o coordenador, que é o mediador que faz parte do grupo. No segundo papel, um corretor itinerante e dois membros de um grupo são intermediados por um mediador de fora do grupo. No terceiro papel, o mediador atua como um representante de seu grupo, ele pode regular o fluxo de informações ou os recursos que saem de seu grupo para o grupo de w. No quarto papel, o mediador v é um porteiro, que pode regular o fluxo de informações ou as mercadorias entrantes para seu grupo provenientes de u. Finalmente, o ligador ou conector – é um ator que faz a mediação entre membros de diferentes grupos, mas que não pertencem a nenhum desses grupos (DE NOOY; MRVAR; BATAGELJ, 2011).

Pode-se concluir que na engenharia social esses papéis de mediação são o que o engenheiro social usa para desenvolver suas técnicas. Ele consegue se colocar em um desses papéis para obter as informações que deseja. Everton (2013) apresenta que os atores sociais não tomam decisões de forma autônoma, como unidade autônoma, mas sim sob fortes influências do comportamento e das escolhas dos outros atores na rede. Soares (2014, p. 57) garante que:

> As medidas de intermediação comparam e medem o proveito que um indivíduo pode tirar de sua posição na rede. Dependendo das ligações que possui e do restante da rede, um indivíduo pode influenciar significativamente no fluxo de informação dentro da rede. [...] Em um contexto de mediação, um indivíduo pode assumir papéis diferentes, de acordo com sua posição em relação aos demais do grupo. O estudo de papéis de mediação geralmente se aplica a situações onde estão envolvidos, dentro de uma mesma rede social a ser analisada, mais de um grupo diferente de atores.

Schneier (2003) assegura que o fenômeno social da *proxy*,[18] quando uma pessoa representa outra, tem profundos efeitos na segurança, e estes *proxys* se tornam livres de qualquer contramedida ou tecnologia empregada na segurança, primeiro porque eles têm o poder de agir como quiserem, principalmente quando visam a seus próprios benefícios, segundo porque não têm a mesma preocupação com a gestão dos riscos que aqueles que representa.

Algo bastante interessante nos conceitos estudados até aqui sobre ARS e o fenômeno de *proxy* e círculo de distância emocional apresentados por Schneier é a convergência para o assunto da confiança entre as pessoas, inclusive sobre engenharia

[18] Um *proxy* é um procurador, um mandatário. Segundo o dicionário Merriam-Webster's, o *proxy* trata do poder ou da autoridade de agir em nome de outro.

social. Se alguém está interessado em elevar os níveis de segurança deve primordialmente entender os interesses dos envolvidos e suas relações com os demais, e isso com certeza é uma questão sociológica. A segurança será sempre um balanceamento entre os interesses dos envolvidos no contexto.

3.5.2 O *software* Pajek

Considera-se muito importante apresentar alguns princípios básicos do uso do *software* de análise de redes sociais. A intenção é prover recursos técnicos para melhor se entender o processo e o método utilizados na pesquisa. Não se pretende ensinar como se utiliza o *software* completamente. Acredita-se ser possível entender o processo de análise das redes coletadas na pesquisa por meio desses conhecimentos.

O Pajek (pronuncia-se paieque) é um *software* esloveno cujo nome significa aranha em esloveno. Alguns conceitos da Teoria dos Grafos são os blocos de construção ou objetos de dados de Pajek. É óbvio que uma rede social é o objeto de dados mais importantes no Pajek. Nele, uma rede é definida de acordo com a Teoria dos Grafos: uma lista de vértices e listas de arcos ou arestas na qual cada arco ou aresta tem um valor. Nas **Figura *32*** e **Figura *33*** estão a tela principal do sistema e sua tela de visualização da rede, para esta segunda tela é necessário utilizar o menu Draw da tela principal.

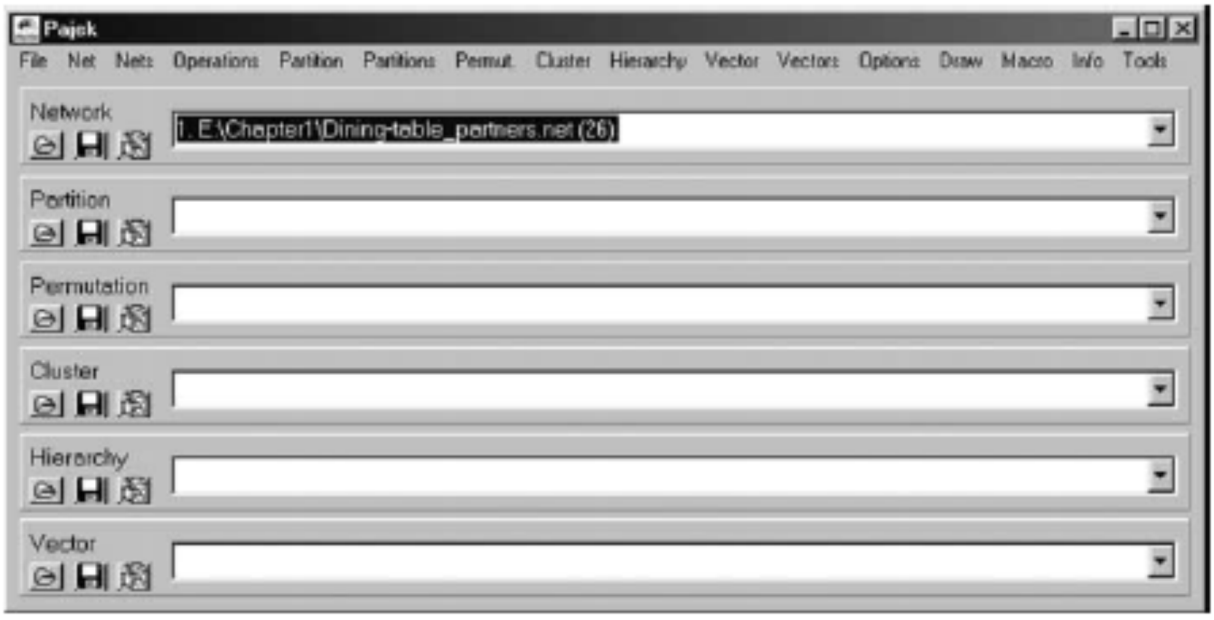


Figura 32. Tela principal do Pajek

Fonte: DE NOOY; MRVAR; BATAGELJ et al. (2011)

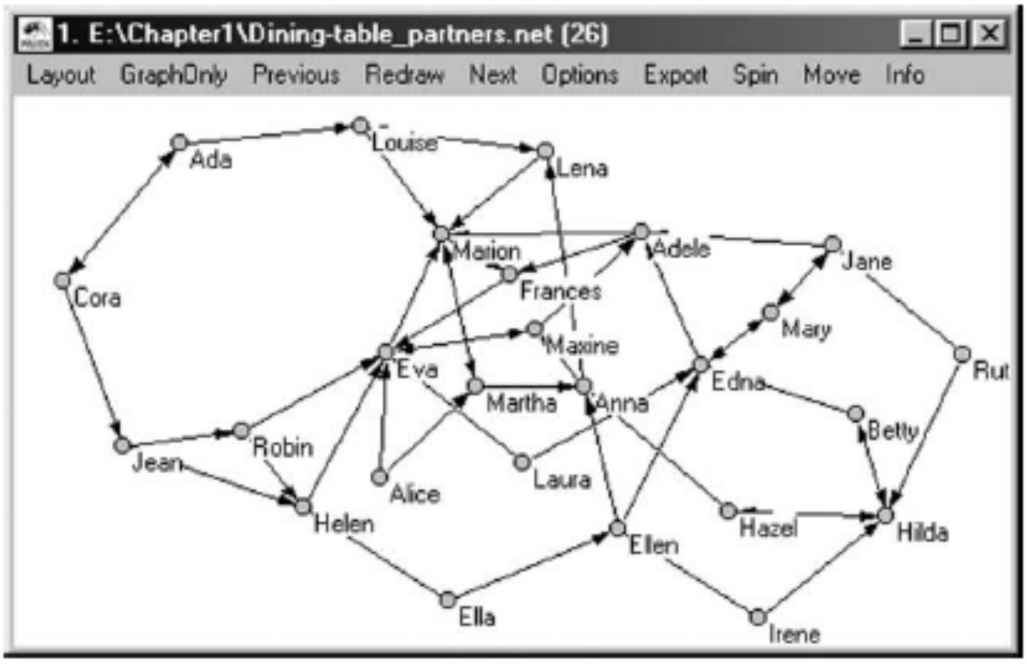


Figura 33. Tela de visualização do Pajek

Fonte: DE NOOY; MRVAR; BATAGELJ et al. (2011)

A entrada de dados no Pajek é feita através de um arquivo do tipo texto. Há um exemplo desse processo na **Figura *34***. A estrutura do arquivo inicia com a posição dos vértices, seguindo para as indicações de conexões direcionadas entre vértices e por fim as conexões não direcionadas.

```
*Vertices  26
   1 "Ada"            0.1646 0.1077 0.5000
   2 "Cora"           0.0481 0.3446 0.5000
   3 "Louise"         0.3472 0.0759 0.5000
   4 "Jean"           0.1063 0.6284 0.5000
[…]
  25 "Laura"          0.5101 0.6557 0.5000
  26 "Irene"          0.7478 0.9241 0.5000
*Arcs
   1   3    2
   1   2    1
   2   1    1
   2   4    2
   3   9    1
   3  11    2
[…]
  25  15    1
  25  17    2
  26  13    1
  26  24    2
*Edges
```

Figura 34. Arquivo de uma rede no Pajek

Fonte: DE NOOY et al. (2011)

Na **Figura *34*** podem ser visualizadas três partes do arquivo: uma para os vértices, outra para os arcos e outra para as bordas (*edges*). No local dedicado aos vértices aparece em cada linha o número do vértice, seguido do nome (*label*) do vértice, seguido de suas coordenadas em um espaço tridimensional. No local dedicado aos arcos aparece um valor numérico para o vértice de origem, seguido do vértice de destino e um valor ou atributo da linha. Por fim, as *edges*, que não levam em conta a direção da linha, na **Figura *34*** não há bordas. Quando uma rede é carregada e se aciona o comando de visualização, pode-se obter algo similar ao que aparece na **Figura *33***.

Após o carregamento da rede no Pajek inicia-se a aplicação de técnicas como transformações, extrações, inserções, classificações, etc. As transformações das redes podem modificar múltiplas linhas e *loops,* além de aplicarem alterações estruturais na rede. Para realizar uma extração, por exemplo, é preciso selecionar um subconjunto de seus vértices e todas as linhas que incidem nos vértices selecionados. Uma partição de uma rede é uma classificação ou agrupamento dos vértices na rede de modo que cada vértice seja atribuído exatamente a uma classe ou um *cluster*.

Para classificar uma rede no Pajek é preciso eleger um número para o *cluster*. No exemplo da **Figura *35*** há os países Algéria, Argentina Austrália e áustria sendo classificados. Pode-se perceber que o valor 2 está agrupando os países Algéria, Argentina e Austrália – que poderia ser uma classificação de acordo com a posição econômica do país. Observa-se também que a Áustria está no *cluster* 1, o que a coloca em um grupo separado dos demais e fará com que ela apareça com uma cor diferente quando o gráfico da rede for desenhado.

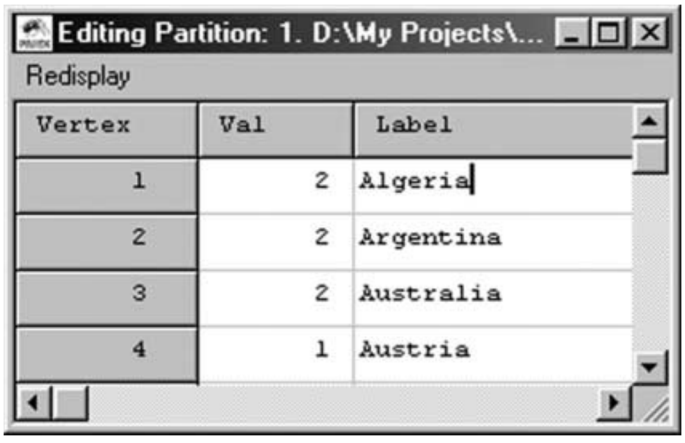


Figura 35. Criando *clusters* no Pajek

Fonte: DE NOOY; MRVAR; BATAGELJ et al. (2011)

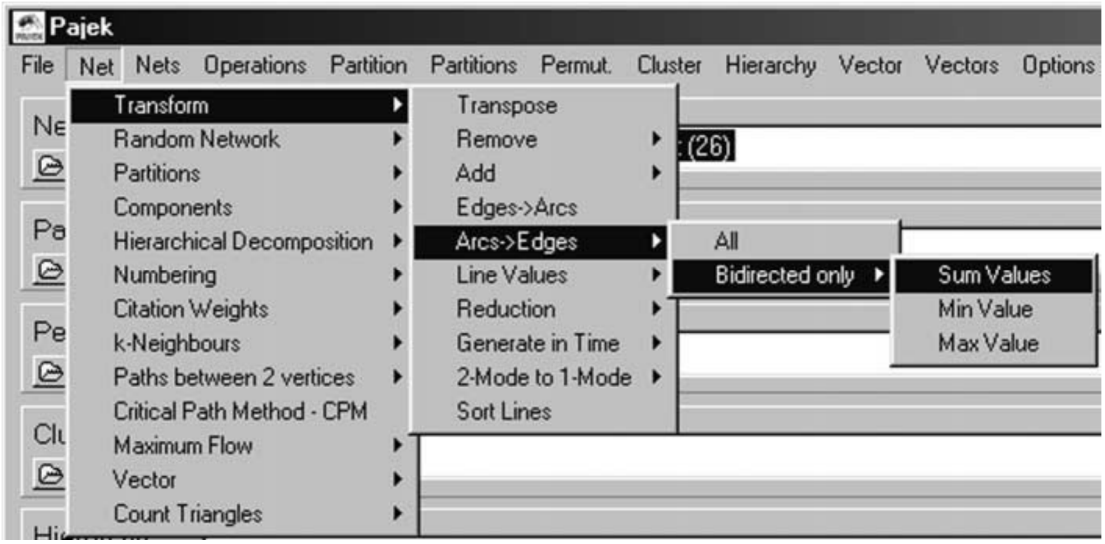


Figura 36. Realizando uma transformação no Pajek

Fonte: DE NOOY; MRVAR E BATAGELJ et al. (2011)

O Pajek pode ser totalmente controlado por meio do seu menu principal. Na **Figura *36*** pode-se observar um exemplo de transformação da rede. O comando a ser executado com base na seleção representada na **Figura *36*** irá transformar a rede direcionada em não dirigida, somando a quantidade de linhas que se repetem em cada relacionamento e colocando o valor como um atributo da linha.

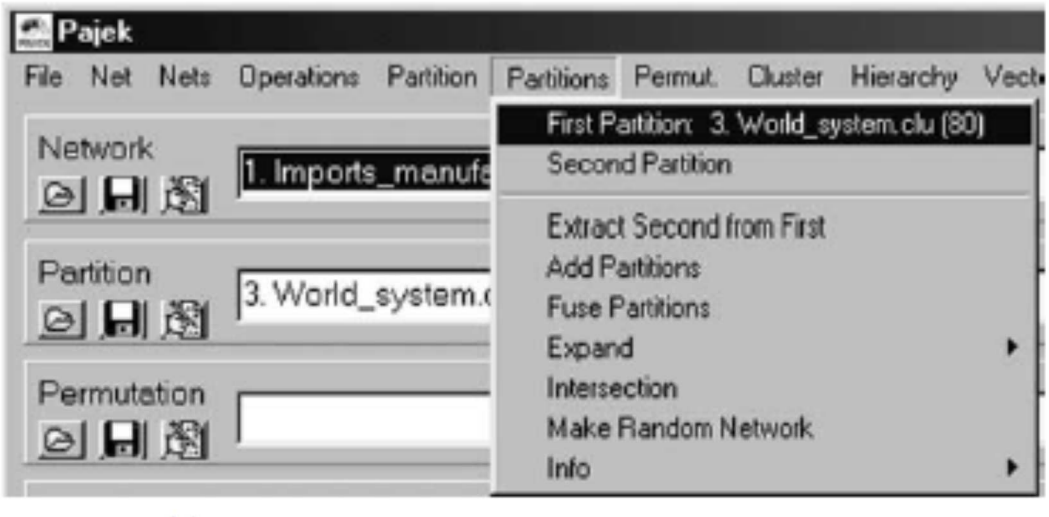


Figura 37. Extração no Pajek

Fonte: DE NOOY; MRVAR E BATAGELJ et al. (2011)

Na **Figura *37*** observa-se no menu Partições (do inglês *Partitions*) uma função de Extração de uma rede através de outras, terceiro menu *Extract Se cond from First*. Quando se tem uma rede menor com vértices que coincidem com uma rede maior é possível extrair daquela rede maior o componente que contém os vértices da rede menor.

Portanto, operações básicas podem ser realizadas nas redes do Pajek. A aplicação de diversas operações básicas ordenadas irá proporcionar insumo analítico. No decorrer da aplicação das transformações, extrações e classificações *insights* podem emergir. Como o arquivo com o qual o Pajek trabalha é no formato texto puro, pode-se utilizar outras ferramentas para auxiliar na análise.

■

Desse modo, a análise de redes sociais é a área conhecida pela investigação das relações e dos vínculos entre os atores sociais, que podem ser pessoas, organizações ou qualquer outra entidade social. Os vínculos, os padrões de comportamento, o fluxo de informação, a ideia e as inovações são circulantes na rede. Os modelos de redes sociais são pontos de vista e promovem ou restringem a visualização de realidade, auxiliando na busca por padrões. A posição dos atores na rede é fundamental para determinar seu papel naquela sociedade. Os modelos de redes sociais materializam uma visão estrutural da rede baseada na relação de seus atores.

3.5.3 Confiança e risco

Gerenciar riscos, administrar incertezas, confiar em alguém ou em alguma tecnologia da informação é algo natural e necessário para as organizações. A confiança, assim como a informação, ainda é um assunto sem definição unificada. Para alguns autores, a confiança é intimamente ligada à incerteza, implicando risco. Para outros autores, seria possível calcular o grau de confiança entre indivíduos.

O fato é que a engenharia social constitui um risco real à segurança da informação e precisa ser discutida. A atuação dos engenheiros sociais se dá por meio do abuso da confiança. Por isso é preciso desmistificar a confiança, que até então seria o “patinho feio” da ciência. Seria muito importante para os estudos de SI e ES poder atuar sobre a confiança com maior controle.

3.5.4 Confiança

Em português, a palavra confiança expressa todas as suas conotações, todos os tipos de confiança. No inglês é diferente. O dicionário Merriam-Webster contempla algumas definições para o termo. Parece que na língua inglesa a confiança é dividida em várias partes, utilizando diferentes termos:

- *confidence*: um sentimento ou consciência do próprio poder;
- *trust:* certeza ou garantia que se tem no caráter, na força ou na veracidade de alguém ou de alguma coisa;
- *reliability*: qualidade ou estado de ser confiável, também traduzido como confiabilidade;
- *trustworthy* (*truth, honesty*): honesto, verdadeiro;
- *trustful*: qualidade de expressar a verdade;
- *dependability*: habilidade de entregar serviço que justificadamente é confiável.

Este trabalho é focado no que podemos chamar de aspecto *trust* da confiança, ou seja, a confiança interpessoal. Portanto, é preciso analisar a confiança tendo em vista o conceito de *trust.*

La Porta, Lopez-de-Silanes et al. (1997) afirmam que a confiança pode não ser verdadeiramente exógena, divergindo das ideias de Fukuyama (2000). Eles definem confiança como um hábito, um comportamento social formado por “associações horizontais

em rede", ou seja, associações de mesma camada social em rede, durante longos séculos da história, entre pessoas, contribuindo para ambas as atividades: comercial e civil. Essas ideias corroboram as ideias de Swan, Cooper et al. (2001), que afirmaram que a confiança é desenvolvida a partir da comunicação e das ações. O grau de confiança é baseado em uma decisão racional (CASTELFRANCHI; FALCONE, 2001).

As ideias de associações em rede e hábitos transmitidos no tempo nos remetem ao conceito de difusão na análise de redes sociais. Quando uma rede está completamente conectada, De Nooy, Mrvar e Batagelj (2011) defendem que é extremamente fácil compartilhar normas, criar confiança e administrar conflitos.

Segundo Huang et al. (2012), outro aspecto importante da confiança é sua dependência do contexto. A confiança sensível ao contexto é composta dos atores envolvidos, do estado das coisas em determinado instante, dos riscos e do grau de comunicação entre as partes. Nessa linha, Schneier (2012) assegura que confiança, no contexto dos seres humanos, não é uma questão de tudo ou nada. Segundo o autor, a confiança na sociedade é contextual e calibrada pela habilidade de se calcular os custos e os benefícios no tempo e no espaço.

Por exemplo:

- Fulano confia que Cicrano faça uma tarefa xyz;
- Beltrano não confia sua senha de acesso nas mãos do seu colega de trabalho;
- Fulano pode confiar em Cicrano hoje, mas pode não confiar amanhã. Assim como Beltrano pode mudar de ideia e confiar sua senha a alguém amanhã.

Claybrook (2004) defende que:

> A confiança é um componente essencial para um negócio a ser realizado. Confiança [...] está relacionado com a compreensão do comportamento interpessoal de um grupo, da eficácia gerencial, do intercâmbio econômico e da estabilidade social e política. (tradução do autor).

Claybook (2004) diz ainda que a confiança é intangível. Então, não seria possível definir confiança formalmente, mais objetivamente? Analisar objetivamente a confiança é analisá-la de forma concreta, e não como algo abstrato. Por exemplo: uma confiança proveniente simplesmente "da alma" ou de uma dimensão ou mundo paralelo, exclusivamente.

Lewicki e Bucker (1996, apud Mcallister, Lewicki e Vedi, 2006) são muito coerentes

ao definir confiança como a expectativa positiva das intenções de outro sobre ele mesmo em uma situação que implica risco. Eles tratam a confiança como tangível e identificam três dimensões distintas para ela: *calculus-based (CBT), knowledge-based (KBT)* e *identification-based (IBT).*

1. CBT – é a confiança baseada no entendimento de que a recompensa e a punição estão bem definidas no relacionamento.
2. KBT – é a confiança nos termos da previsão e da dependência. Esta requer mais informações da outra parte e provém de uma comunicação regular.
3. IBT – é a confiança fundamentada na internalização e no entendimento profundo das intenções e dos desejos do outro. Esse é o estágio mais avançado da confiança e surge em poucos casos.

Pode-se observar que o CBT é uma medida construída por elementos exógenos. Por sua vez, o KBT e o o IBT são também provenientes de fontes exógenas, vindas das interações humanas, mas com uma forte dimensão endógena e, o que é mais interessante para este estudo, são provenientes da comunicação. As duas são produto do aprofundamento das relações sociais por meio da comunicação.

Na teoria de Shannon, segundo Rezende (2011), informação é o que é transferido de um ponto a outro por um canal de comunicação. Para o autor, como fronteira conceitual na ciência, “confiança” parece ser algo de difícil definição, até mais do que as ideias de tempo e espaço. Rezende recorda do estigma da confiança ser subjetiva e imprecisa.

Gerck (1998, apud REZENDE, 2011) situa a noção de confiança naquilo que é esperado e entendido pelo receptor. Em seu trabalho pioneiro, Gerck define confiança nas comunicações como aquilo que é essencial para um canal[19] de comunicação, mas que não pode ser transferido da fonte para o destino através desse canal.[20]

---

[19] É importante recordar das ideias de Tubbs, que defende que a total efetividade da comunicação exige um clima psicológico positivo e de confiança. A convergência é empolgante quando se pensa nos modelos de Drestke, Gerk e Tubbs e nos conceitos de homofilia de Lewicki e Bucker. Pois à medida que se conhece o outro e há uma identificação surge o fenômeno da homofilia e o *Inforational Link* se manifesta, dentro de um contexto de comunicação e confiança. Isso pode levar à conclusão perigosa de quantificar a confiança pela quantidade de comunicação.

[20] Se pensarmos nos estudos de Gumpert et al. em 1990, que tratavam a mediação das comunicações como um estudo sobre os indivíduos, sendo seus papéis na comunicação entrelaçados entre emissor, receptor e canal de comunicação. Observa-se que se a confiança é inerente ao canal e que se o ser humano pode ser parte do canal, nada mais claro que defender que ao se estudar as comunicações e a confiança no propósito de controlá-la está se estudando a mediação das comunicações. Acredita-se que o estudo de Gerck convirja para a definição de *Informational link* de Dretske.

O conceito de confiança de Schneier (2012) é complexo e engloba diversos significados. A ideia do autor é que o fenômeno da confiança está ligado à questão das futuras ações de contingência, consequência das ações de outros. Esse conceito expressa que o estabelecimento da confiança envolve bom senso sobre as ações de outros que possam afetar nossos interesses.

Portanto, Schneier analisa confiança sob o aspecto das relações interpessoais. Afirma ele que, ao confiarmos em alguém, também confiamos nas ações e nas intenções daquele em quem confiamos. Por exemplo: podemos confiar que outro cidadão não irá atravessar o sinal vermelho no trânsito e, assim, o trânsito, como um todo, torna-se mais confiável.[21]

Outro exemplo seria: a participação da confiança no mundo corporativo e nos contratos. Segundo Schneier (2012) ensina, o contrato é um mecanismo institucional para fortalecer a confiança entre as partes que dele participam. O contrato seria uma materialização do CBT de Lewicki e Bucker em uma relação social.

A segurança gira em torno das pessoas e é geralmente dependente delas. A pessoa confiável – aquela da qual o sistema depende para funcionar – é parte do sistema de segurança. Ela é um elemento crítico para os sistemas de segurança, porque o ser humano geralmente é o elemento mais resiliente de um sistema, sendo hábil para decidir e mudar o curso de uma situação (SCHNEIER, 2003).

Schneier (2003) considera ainda que, com certeza, o ser humano é uma espada de dois gumes, ele pode cair no sono, ele pode se distrair, ele pode ser enganado, etc. Segundo o autor, a mente humana seria a melhor contramedida para manter a resiliência do sistema. Em contrapartida, as pessoas são, em muitos casos, o elo mais fraco da segurança e a causa da sua falha. Ele afirma que um bom sistema de segurança retira o melhor das pessoas, prevenindo-se dos abusos de confiança que podem ocorrer.

Schneier (2012) apresenta as três funções críticas da confiança:

1) tornar a sociedade mais previsível;
2) criar o senso de comunidade;
3) tornar mais fácil o trabalho em equipe.

As **Figura *38*** e **Figura *39*** apresentam uma rede social – sociograma – dirigida com

[21] A segurança e a efetividade do trânsito nos cruzamentos dependem da confiança, pois cruzamentos são atravessados em alta velocidade com pouca preocupação de colisão.

pesos, que poderia representar a confiança discreta e probabilística entre os atores Pedro, Maria, Jacó, João e José, respectivamente.

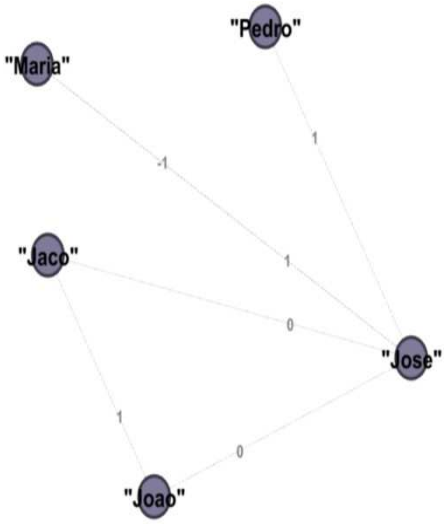


Figura 38. Grafo com pesos discretos (sociograma)

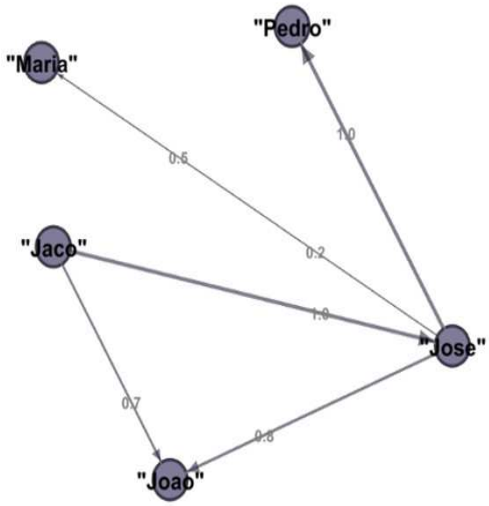


Figura 39. Grafo com pesos probabilísticos (sociograma)

Guha et al. (2004) esclarecem que uma rede dirigida, de pessoas conectadas com pesos ou *scores* de confiança, pode representar uma teia de confiança (do inglês *web of trust*). Eles apresentam um modelo de previsão das relações de confiança com base em uma rede preestabelecida. Os pesquisadores informam que a confiança é propagada por meio das relações sociais. Eles recordam do sucesso do *software Pretty Good Privacy* (PGP), um dos primeiros trabalhos que utilizaram uma teia de confiança.

Abdessalem, Cautis e Souhli (2010) apregoam que os modelos de confiança se dividem em Modelos de Confiança Discretos e Modelos de Confiança Probabilísticos. Nos Modelos de Confiança Discretos, **Figura *38***, a declaração de confiança pode ser positiva (1) ou negativa (-1) – o valor zero (0) define que não há declaração de confiança para a relação social. Nos Modelos de Confiança Probabilísticos, **Figura *39***, são utilizados cálculos estatísticos, e geralmente a confiança e a desconfiança são representadas por valores no intervalo de -1 e 1. Os Modelos de Confiança Discretos podem ser entendidos como simplificações.

Silva e Ferreira (2007, p. 8) alegam que as relações de confiança existentes na rede são fundamentais para o papel do intermediário. Em razão da limitada capacidade de processamento da informação pelos indivíduos (racionalidade limitada), a qualidade da

informação recebida não pode ser integralmente verificada, assim sua qualidade depende da reputação das fontes.

Abdessalem, Cautis e Souhli (2010) classificam os trabalhos recentes na administração das teias de confiança em duas famílias: os que abordam a inferência da confiança levando em consideração a inteligência artificial – *machine learning;* e os baseados nas interações prévias dos usuários, chamados de *predictives* (proféticos) – cuja abordagem é a propagação da confiança.

Huang et al. (2012), baseados em seus experimentos com redes sociais, afirmam que se pode intuir que pessoas semelhantes, ou com os mesmos traços de personalidade, que se identificam tendem a confiar umas nas outras. Continuam afirmando que pessoas que confiam em determinado indivíduo preferirão confiar nos indivíduos nos quais este confia. A afirmação anterior remete ao conceito de homofilia da ARS.

Recordando, De Nooy, Mrvar e Batagelj (2011) definem a homofilia como a tendência de os similares interagirem entre si com mais intensidade que os dissimilares.[22] Schneier (2012), na **Figura *40***, modela círculos de distância emocional e defende a influência desses círculos[23] no estabelecimento da confiança.

Schneier (2012) informa que somos mais propensos a confiar em pessoas similares a nós – o que se pode entender como homofilia: pessoas que se vestem como nós, agem como nós, parecem conosco e falam como nós, por exemplo: confiamos mais em nossos familiares do que em pessoas estranhas a esse círculo. Tendemos a generalizar as relações, por exemplo: se tivemos uma boa experiência em um país com um estrangeiro tendemos a generalizar; se tivemos uma má experiência com algum estrangeiro, também tendemos a generalizar.

[22] No contexto da segurança da informação, essas afirmações são muito interessantes, por que quando o engenheiro social se passa por alguém utilizando jargões técnicos de uma comunidade e informações, ele está se colocando numa posição de igualdade para, provavelmente, explorar o fenômeno da homofilia.
[23] Aqueles considerados iguais, mais próximos são mais confiáveis. Quanto mais próximos dos círculos de interesses pessoais, mais confiança pode ser criada entre indivíduos, afinal, entre próximos há pouca competição. Se não há competição é provável que haja colaboração. Interesses iguais facilitam a cooperação entre as partes.

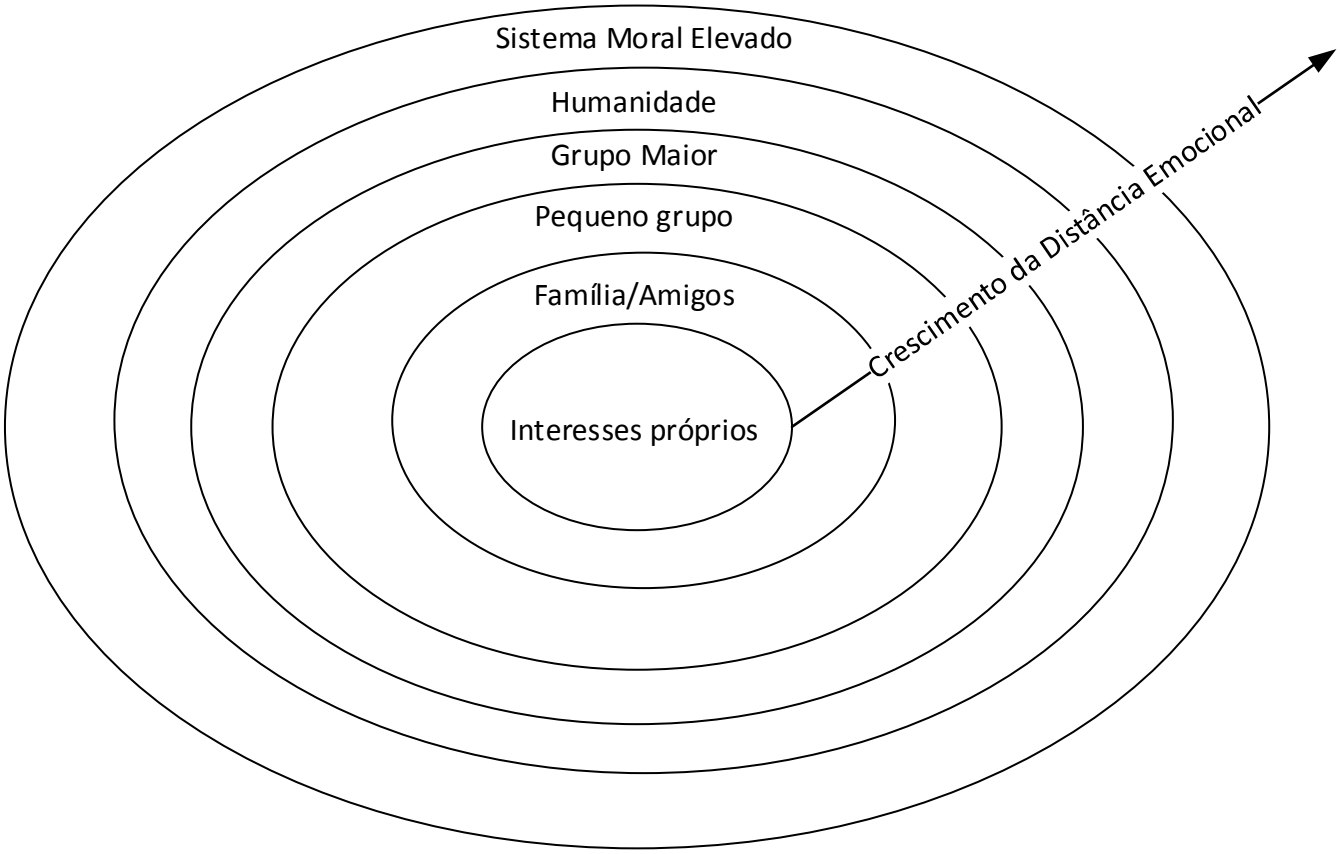


Figura 40. Distância emocional

Fonte: SCHNEIER (2012, p. 143; tradução do autor)

Com isso pode-se defender que a confiança é um fator gerador de riscos, e se o cerne da segurança da informação é administrar riscos, então a engenharia social é uma questão da administração de riscos. Logo, o abuso de confiança é o ponto fulcral da segurança da informação. A questão maior a ser levantada é que a confiança está intimamente ligada à incerteza.[24] Ao se analisarem as relações sociais de confiança caso a caso, pode-se calcular o grau aproximado de confiança entre os indivíduos.

[24] Se não há incerteza não há confiança. Imagine-se um caso hipotético de controle total entre indivíduos, por mais que pareça impossível, cada ação de um determinado indivíduo é previsível. Ao se transferir qualquer objeto a este indivíduo controlado, não se está confiando a ele nada. A confiança presume liberdade. Portanto, os cenários de confiança podem ser controlados e mediados.

3.5.5 Risco

Risco e confiança estão intimamente associados. Nesta seção são abordados o risco e sua relação com a confiança. Defende-se que a modelagem dos riscos e da confiança é possível, talvez por meio de proposições lógicas, talvez por meio da ARS. Percebe-se que sua grandeza quantitativa e sua importância qualitativa se complementam. Mas são necessárias ações sociais práticas para arquitetar essa modelagem e enfrentar o desafio de entender esses fenômenos intrincados. A seguir, algumas proposições:

- Fulano confia ao Cicrano seus segredos íntimos; Fulano assume o risco de Sicrano contar seus segredos a alguém.
- Beltrano confia sua vida nas mãos do paraquedista em um salto duplo, logo, Beltrano assume o risco de o paraquedista falhar e eles perderem suas vidas.

Quem confia mais em quem? Fulano confia mais em Cicrano ou Beltrano confia mais no paraquedista? Isto é certo: se dentro do contexto o valor da vida for maior que os segredos íntimos, Beltrano é o ator que mais confia no outro. De forma geral, é possível perceber a grandeza da confiança por meio da análise de proposições e do contexto do risco. Assim, entender o que é o risco e sua relação com a confiança é fundamental.

Afinal, o que é um risco? Para Fernandes (2010b), um risco é uma estimativa da incerteza e das consequências relacionadas à ocorrência de um evento indesejável. Por sua vez, Coso (2007) afiança que o risco é representado pela possibilidade de um evento ocorrer e afetar negativamente a realização dos objetivos organizacionais. Fernandes (2010b) doutrina que um risco de segurança é um evento possível e potencialmente danoso a uma organização. Seria um evento improvável, que possui chance de acontecimento futuro, que não é nula, e que apresenta impacto negativo significativo. Fernandes explica que a gestão do risco de segurança é um elemento orientador das decisões no domínio da segurança, que “o principal processo decisório na segurança da informação consiste em decidir quais tratamentos serão dados aos riscos levantados, estimados e priorizados por meio de processos sistemáticos de coleta de informações e diálogo reflexivo”. Ele afirma que os controles de segurança da informação são inseridos no processamento da informação organizacional de forma justificada e planejada com base na gestão do risco de segurança.

Schneier (2003) garante que quando se fala em risco nessa disciplina está se

tratando da probabilidade de uma ameaça virar um ataque real e bem-sucedido sobre a informação. Por sua vez, a administração de riscos é a querela sobre a quais riscos devem ser aplicadas contramedidas e quais riscos podem ser ignorados. Desse modo, ameaças, para o catedrático, determinam riscos, e os riscos determinam contramedidas, ou seja, proteções, controles de segurança.

A norma ISO 31000 (ABNT, 2009) define risco como o efeito da incerteza nos objetivos. Na norma, o efeito é um desvio em relação ao esperado – positivo e/ou negativo. Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde, de segurança, ambientais...) e podem ser aplicados em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo). Para Coso (2007, p. 14):

> Uma premissa subtendida do gerenciamento de riscos é que **toda organização, seja ela com ou sem fins lucrativos ou órgão de governo, existe para gerar valor para as partes interessadas**. Todas as organizações enfrentam incertezas, **e o desafio da direção é determinar o nível de incerteza que ela está preparada para enfrentar** na medida em que se empenha para aumentar o valor para as partes interessadas. **As incertezas geram riscos** e oportunidades, com potencial para destruir ou gerar valor (grifo nosso).

Para a ISO 31000, o risco é muitas vezes caracterizado pela referência aos eventos potenciais e às suas consequências, ou uma combinação destes. O risco é muitas vezes expresso como uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada. A incerteza é o estado, mesmo parcial, da deficiência das informações relacionadas a um evento, sua compreensão, sua consequência ou sua probabilidade, conhecimento.

Mäkinem (2005) afirma que, de forma geral, o alvo do gerenciamento de riscos – ambos os eventos: econômicos ou de segurança – é o controle das ameaças, que é encontrado quando a organização ou a sociedade especificam as consequências e as probabilidades das ameaças.

Pode ser observado na ABNT 31000 (2009, p. 8) que o sucesso da gestão de riscos dependerá da eficácia da própria gestão do órgão, que fornece os fundamentos e as disposições que irão institucionalizá-la em toda a organização, em todos os níveis. A boa gestão de riscos de segurança da informação, para Fernandes, passa pela minimização ou pela eliminação do impacto dos incidentes de segurança da informação.

Castelfranchi e Falcone (2001), em sua abordagem cognitiva da confiança, estabelecem que confiar é arriscar-se, assim, confiar implica risco. Dizem eles que o grau

de confiança é baseado em decisão racional, mas confiar requer a aceitação de riscos. Hill e O'Hara (2005) lecionam:

> A confiança é um componente essencial das relações humanas e um alicerce fundamental das sociedades saudáveis. Apesar de sua importância, estudiosos de várias disciplinas relevantes para a confiança têm falhado ao tentar convergir para uma única definição. Muitos especialistas na área parecem concordar que a confiança é um estado de espírito que permite que seu possuidor esteja disposto a fazer-se vulnerável a outro, isto é, confiar no outro, apesar de um risco positivo que o outro possa agir de uma forma que possa prejudicar (tradução do autor).

Pode-se inferir que se confiança implica risco, não há de se falar em confiança sem estudar, mesmo que superficialmente, o risco. O risco é a possibilidade de algo dar errado, resultar em um problema e não em uma solução. Quanto se aplica uma ação, o risco está na possibilidade de essa ação ser danosa e prejudicial. Se a confiança é ligada à incerteza e o risco é a possibilidade de resultado negativo, pode-se pensar em um estado de confiança que não resulte em resultado positivo, logo implica risco. Enfim, o risco de uma confiança inapropriada deve ser analisado.

Portanto, confiança como um hábito, comportamento social, formada por "associações horizontais em rede" é baseada em uma decisão racional. Para uma percepção da confiança em seu contexto é preciso inteligência – é preciso compreender e conhecer o conflito de interesses para, então, inferir a confiança atribuída às partes. Confiança é sua dependência do contexto e, provavelmente, é tangível. Com os controles adequados pode-se mediar a confiança interpessoal em um instante, talvez se utilizando modelos de confiança discretos ou/e probabilísticos. A confiança é necessária nas comunicações, e a mente humana seria a melhor contramedida, pois tem a capacidade de discernir o risco que determinada confiança promove. Somos mais propensos a confiar em pessoas similares a nós. Tem-se de manter a resiliência do sistema, por isso a confiança nas pessoas tem de vir acompanhada de uma gestão de risco adequada.

4 Resultados

4.1 Análise dos dados e discussão

Esta subseção está dividida em apresentação dos dados, método analítico e discussão. Nas subseções 4.1.1, 4.1.2 e 4.1.3 são apresentados os dados e os métodos analíticos. Na subseção 4.1.4 encontra-se a discussão sobre os dados, com um cruzamento dos pressupostos. As conclusões estão na subseção 4.2.

4.1.1 Primeira bateria de coletas dos dados

Após a execução de várias baterias de coleta sobre 25 órgãos superiores do governo, por exemplo: Presidência da República, Ministério da Educação, Ministério dos Esporte., e sobre 314 outros órgãos, por exemplo: secretarias, institutos, universidades, agências reguladoras. Por fim, a execução da pesquisa ocorreu sobre 4.275 unidades gestoras (UGs) de gastos públicos.

A varredura ocorreu em grande quantidade de dados e em aproximadamente dois meses de execução do *script* para dois meses de dados varridos. Houve muitos ajustes no robô, que ainda está longe do estado da arte. Foram coletados no Portal da Transparência 275 registros sobre aquisições relacionadas à tecnologia da informação.

Executou-se outro *script* para transformar os dados em redes sociais que o Pajek pudesse manipular. Essas redes são de dois modos: uma contém os favorecidos e outra, as unidades gestoras. Na **Figura *41*** está o primeiro sociograma encontrado – a cor amarela refere-se à UG, e a cor verde, ao favorecido do contrato:

Aqui se inicia a análise de redes sociais. Foi aplicado um algoritmo de alteração de *layout* – que o Pajek oferece – baseado em energia chamado Kamada Kawai. Foi trocada a indicação do vértice por números para melhor visualizar a rede social. A rede está apresentada na **Figura *42***. A rede transformada proporcionou uma visualização e uma análise melhores. A rede da **Figura *41*** e a da **Figura *42*** têm a mesma topografia, apenas o *layout* foi alterado.

Pode ser observado que a rede social em análise possui muitos componentes, os quais foram organizados no espaço. No sistema Pajek isso é possível arrastando-se e soltando-se com o ponteiro do *mouse*. Os vértices foram deslocados um a um para uma posição na qual não houvesse cruzamentos entre eles, sendo que o resultado está na **Figura *43***.

.

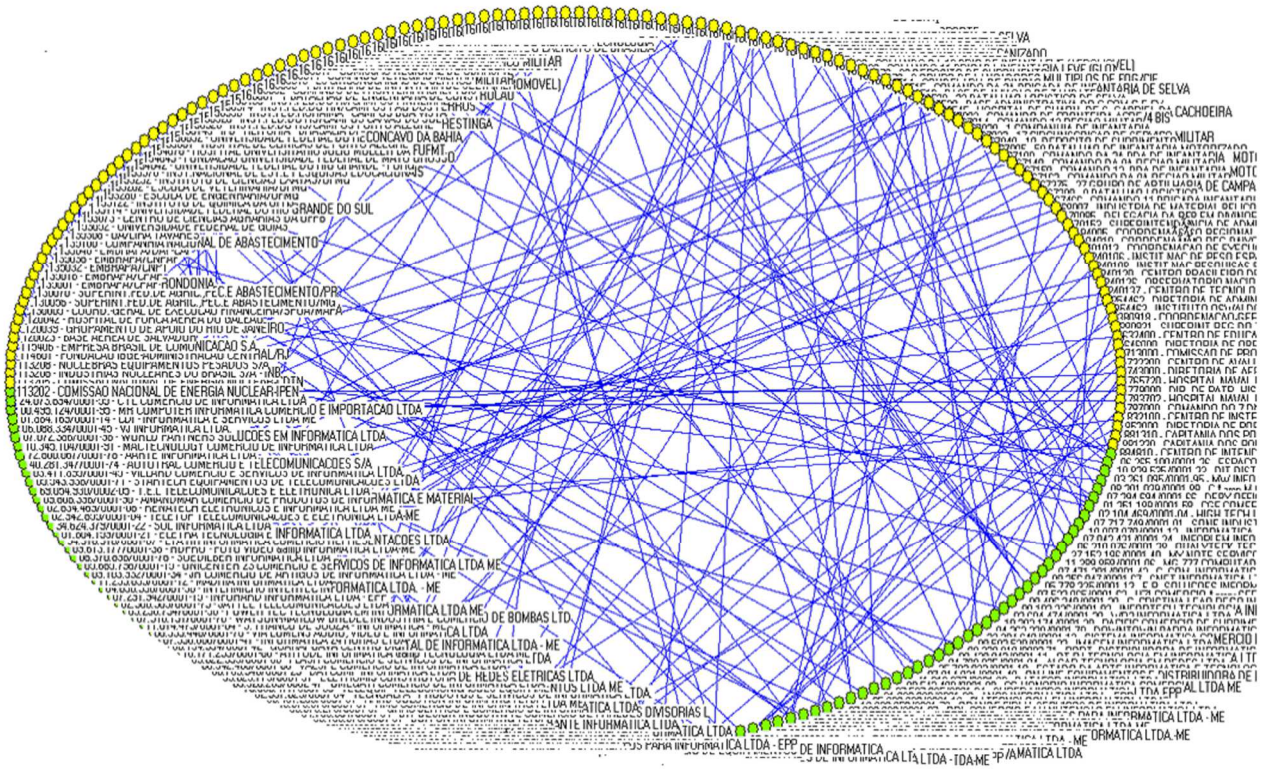


Figura 41. Sociograma da extração do Portal da Transparência

A partir desse ponto optou-se por selecionar apenas os componentes com mais de três vértices para assumir alguns dos papéis de corretagem em análise de redes sociais. Dessa forma, foi utilizada a técnica de criação de uma partição pelo número de vértices, tendo sido extraídos os maiores que 3.

Na **Figura *44*** pode-se observar o efeito da aplicação da terceira técnica de análise de redes sociais. Destacam-se os componentes com mais de três vértices. Os vértices de cor branca são aqueles que têm dois vértices. Na **Figura *45*** encontra-se a rede transformada a partir da extração dos componentes com menos de dois vértices. Os componentes isomorfos foram agrupados para que se pudessem trabalhar cenários e ataques por tipo de relação de comunicação e confiança. Podem-se observar as estruturas do fluxo de informação, similares às apresentadas por Baker na comunicação informal.

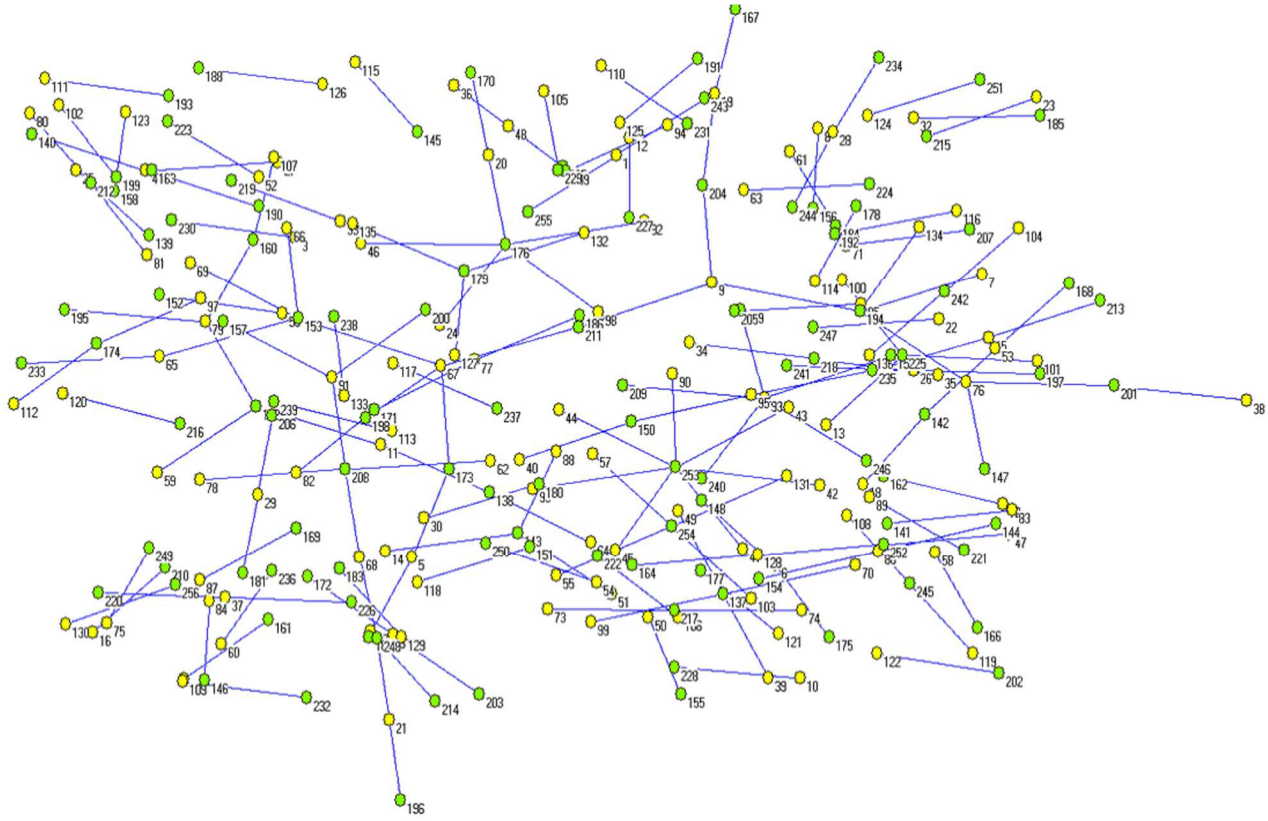


Figura 42. Rede extraída e com primeira transformação

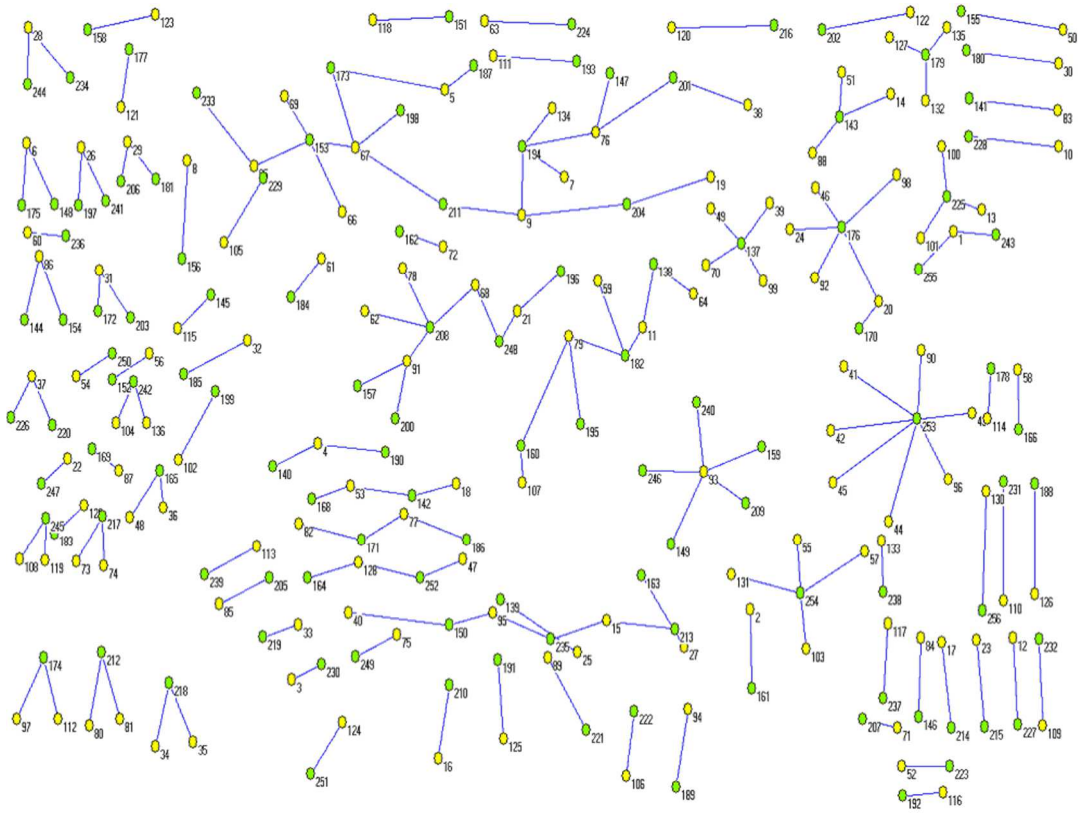


Figura 43. Organização dos componentes, segunda transformação

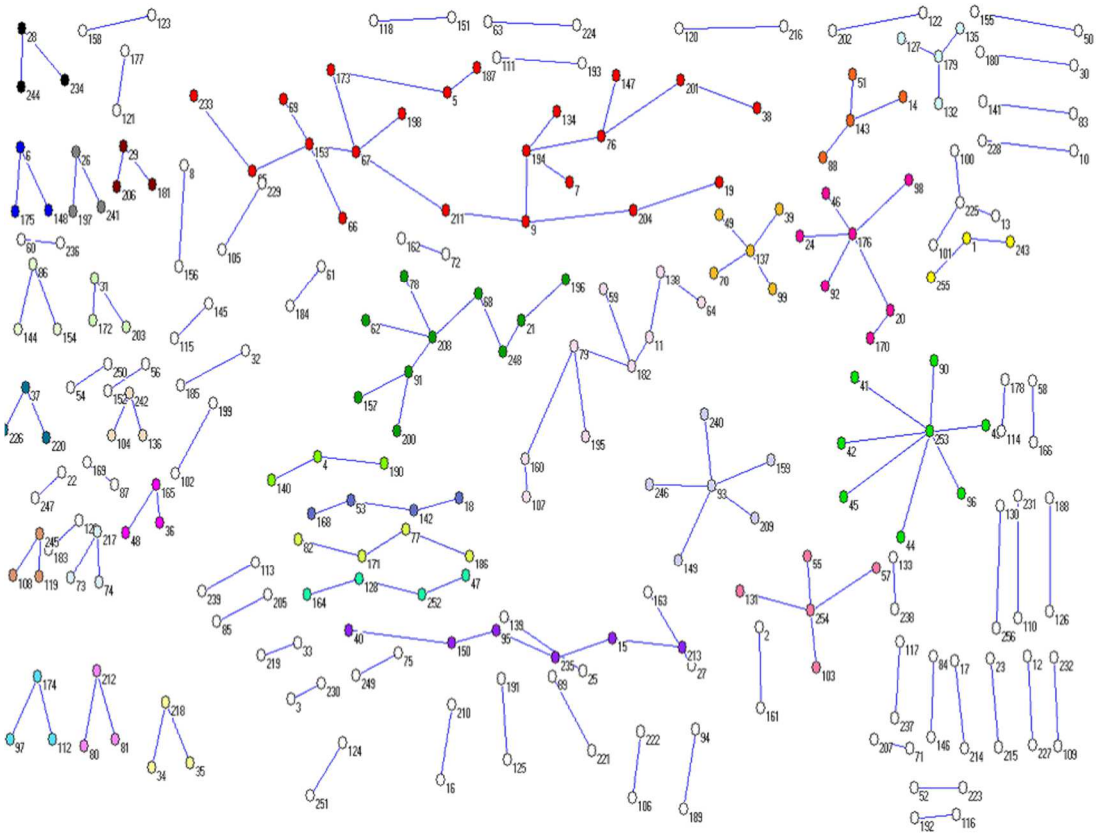


Figura 44. Componentes com mais de dois vértices destacados

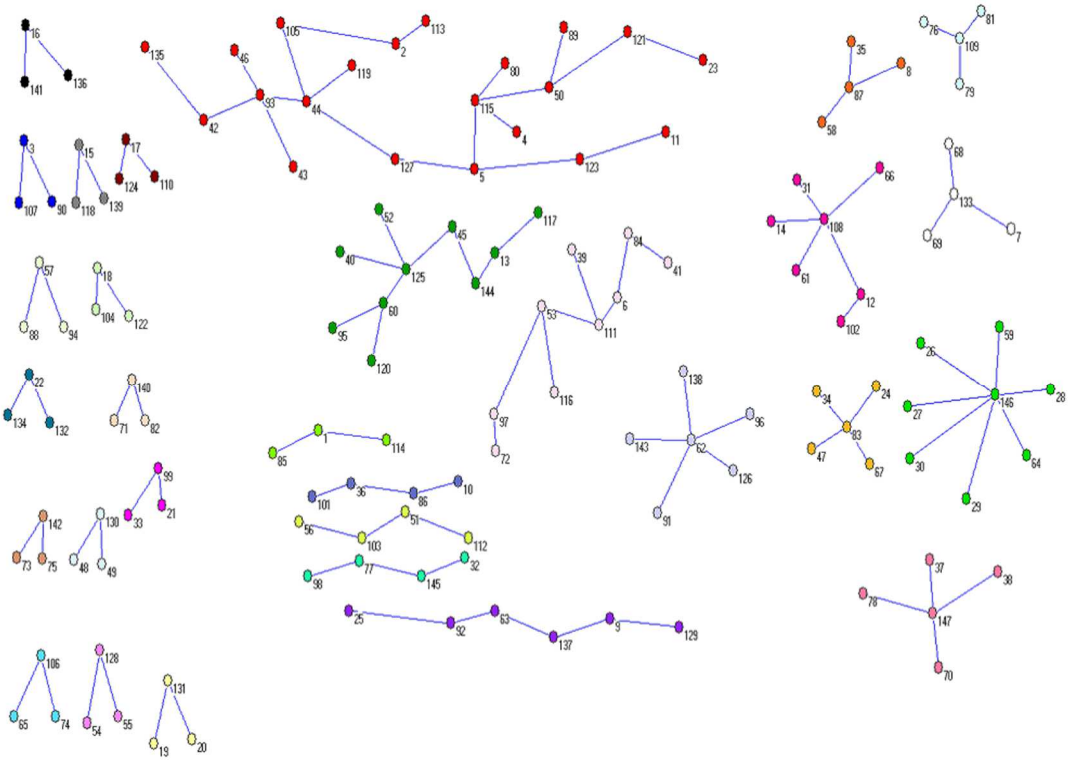


Figura 45. Extração dos componentes com mais de dois vértices

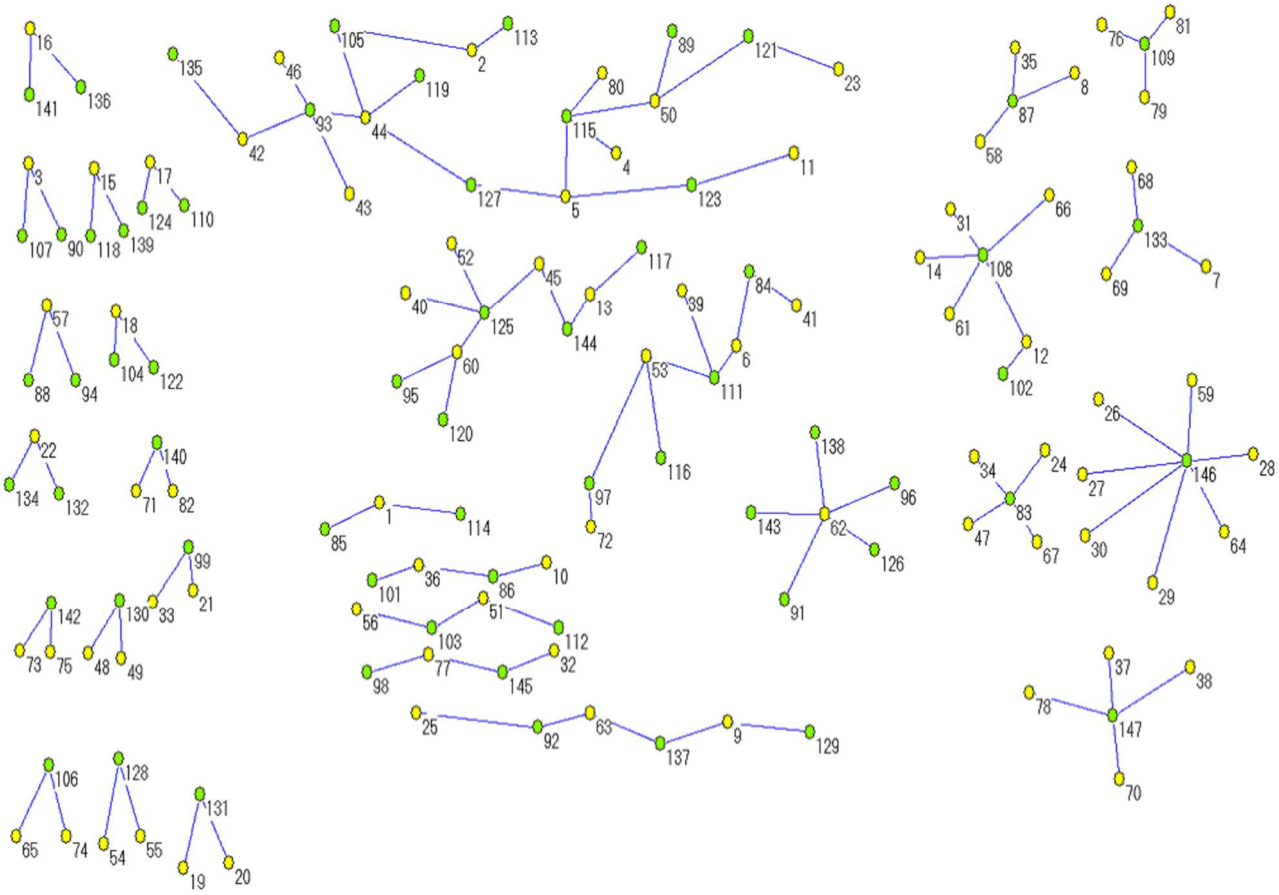


Figura 46. Componentes apresentados com partição de UG/favorecido

Aplicaram-se os componentes à partição, que divide os nós em unidades gestoras e favorecidos nos contratos. Aqui fica claro que uma organização pública pode relacionar-se com outro ator de formas diferentes, ora assumindo um papel, ora outro. Lembre-se que os vértices de cor amarela são a UG e os de cor verde são os favorecidos.

Observe-se agora o caso do componente com os vértices 134, 132 e 22. Na **Figura *46*** pode ser observado que ele faz parte do *cluster* 18. Se for utilizado o método de análise de redes sociais para a extração de componentes a partir de uma partição será obtido o componente presente na **Figura *47***. Nessa figura tem-se o componente 18, com seus rótulos apresentando o nome da organização que este nó representa e as cores com a partição UG/favorecido.

Pode-se afirmar, sucintamente, que a Instituição Federal do Rio Grande do Norte/Campus Pau dos Ferros, destacada na **Figura *47*** com código da UG 158374, poderia ser um alvo para ataque similar ao apresentado nas páginas 88-92, em que uma organização alvo tem relação de confiança, aqui podemos dizer contrato de prestação de

serviço, com duas organizações privadas. O atacante pode se passar por funcionário das duas organizações privadas em situações diferentes a fim de abusar da confiança de algum servidor ou contratado bem-intencionado.

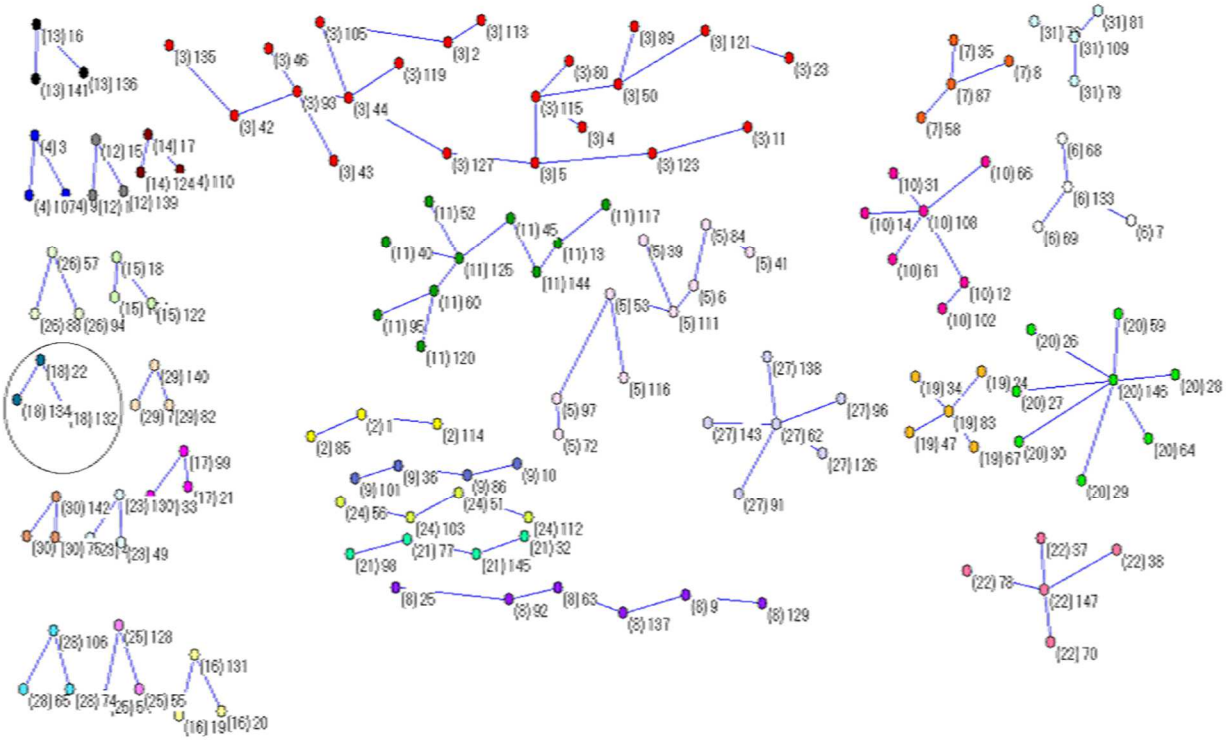


Figura 47. Componentes marcados com o valor do *cluster* ao qual pertencem

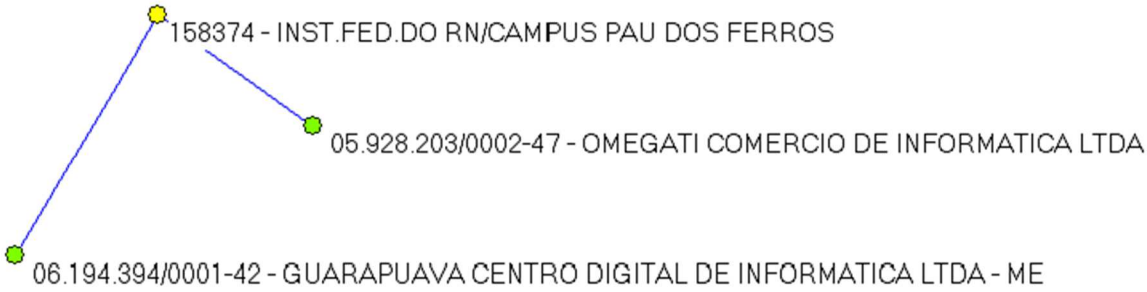


Figura 48. Componente 18 – um caso para ser explorado

Na subseção 4.1.4 os dados serão mais bem discutidos.

4.1.2 Segunda bateria de análise dos dados

Para validar o método estudado e dar maior solidificação científica ao trabalho, resolveu-se executar o processo novamente focando em instituições do Distrito Federal.

Foram realizadas algumas entrevistas para se ter outro tipo de fonte de dados. As entrevistas foram outro mecanismo utilizado com o intuito de aumentar a credibilidade das conclusões do estudo.

Foram coletados 6.943 registros do Portal da Transparência. Retiraram-se apenas os registros que continham data superior ou igual a 01/01/2014. Foram 122 registros, que poderão ser detalhados utilizando-se a análise de dados a seguir.

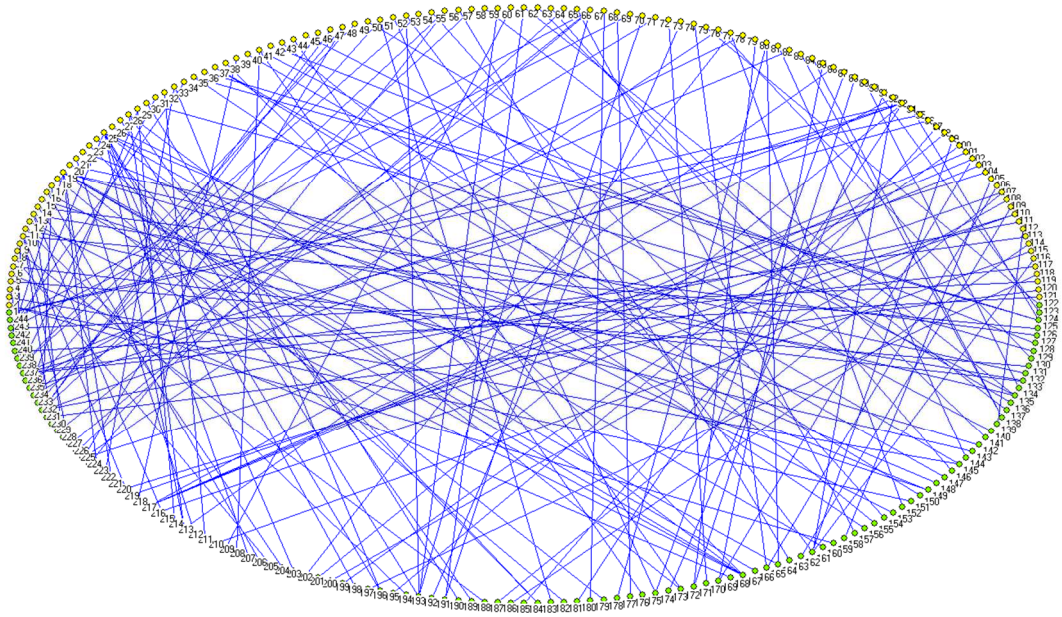


Figura 49. Rede contendo apenas registros coletados em 2014

Da mesma forma como o que foi feito anteriormente, primeiramente é alterado o *layout* da rede de circular para Kamada Kawai. Como pode ser visto na Figura 50, a rede é organizada em componentes isomorfos. Em seguida, Figura 51, foi criado um particionamento considerando-se componentes com uma quantidade de nós maior que 3.

Após a extração dos componentes com quantidade de nós menor que 2, foram selecionados quatro componentes, que foram separados na parte inferior da **Figura *52***. Para verificar cada caso, os rótulos foram habilitados para cada nó. Pode ser observado, **Figura *53***, que quando os rótulos são habilitados a visualização fica comprometida. Portanto, foram extraídos os quatro componentes inferiores para que pudessem ser analisadas com mais clareza as situações de identificação de alvo para golpes decorrentes de engenharia social.

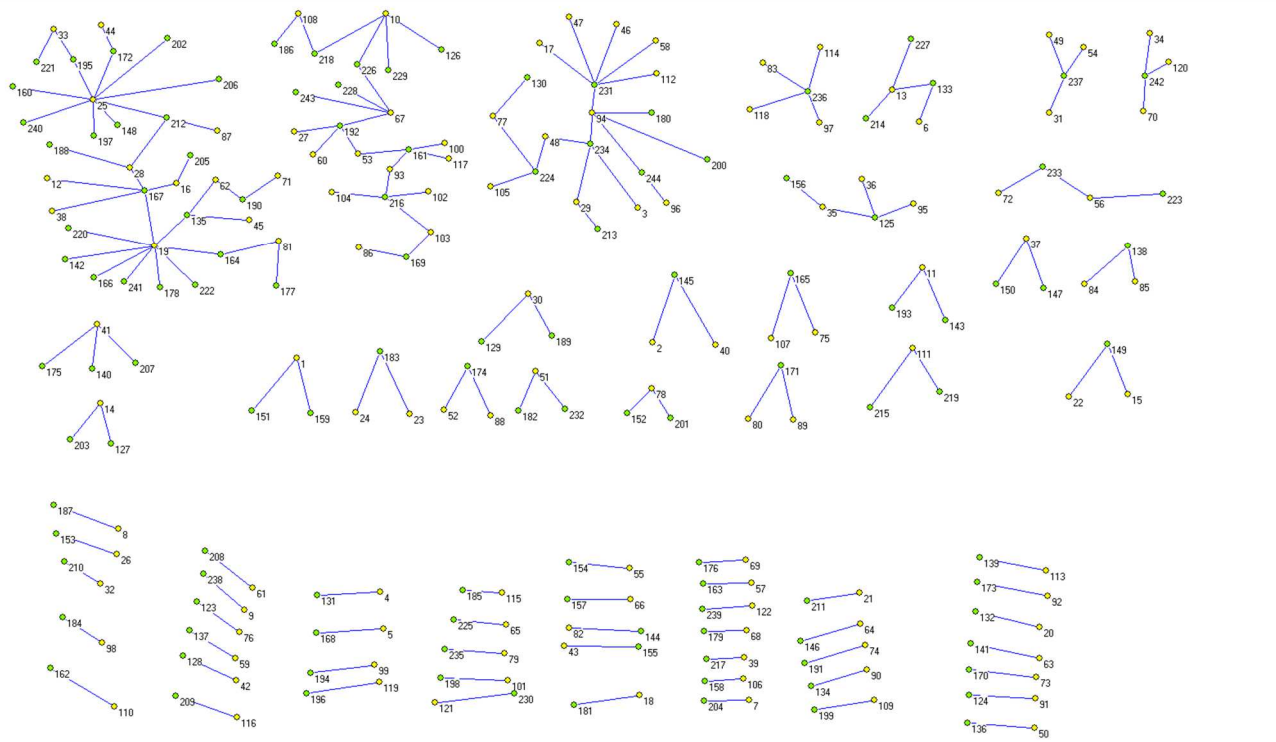


Figura 50. Rede organizada em componentes isomorfos

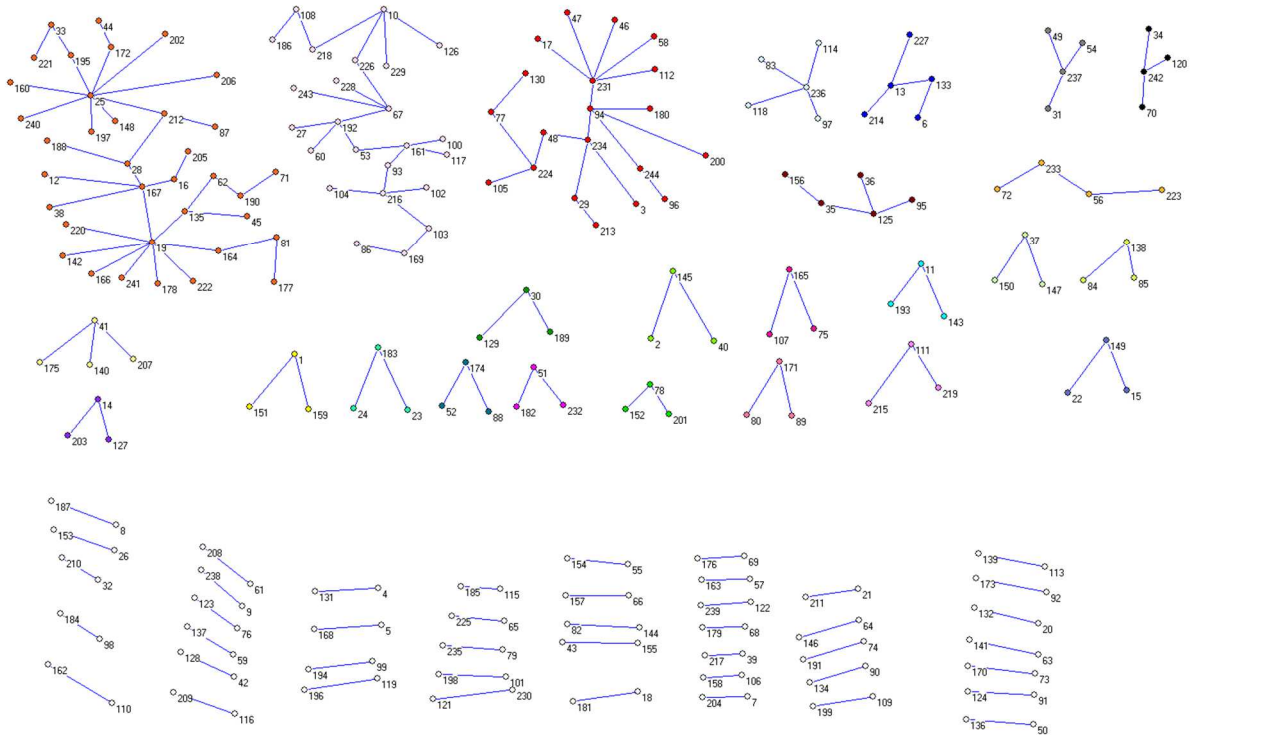


Figura 51. Criação de partição com componentes maiores que dois nós

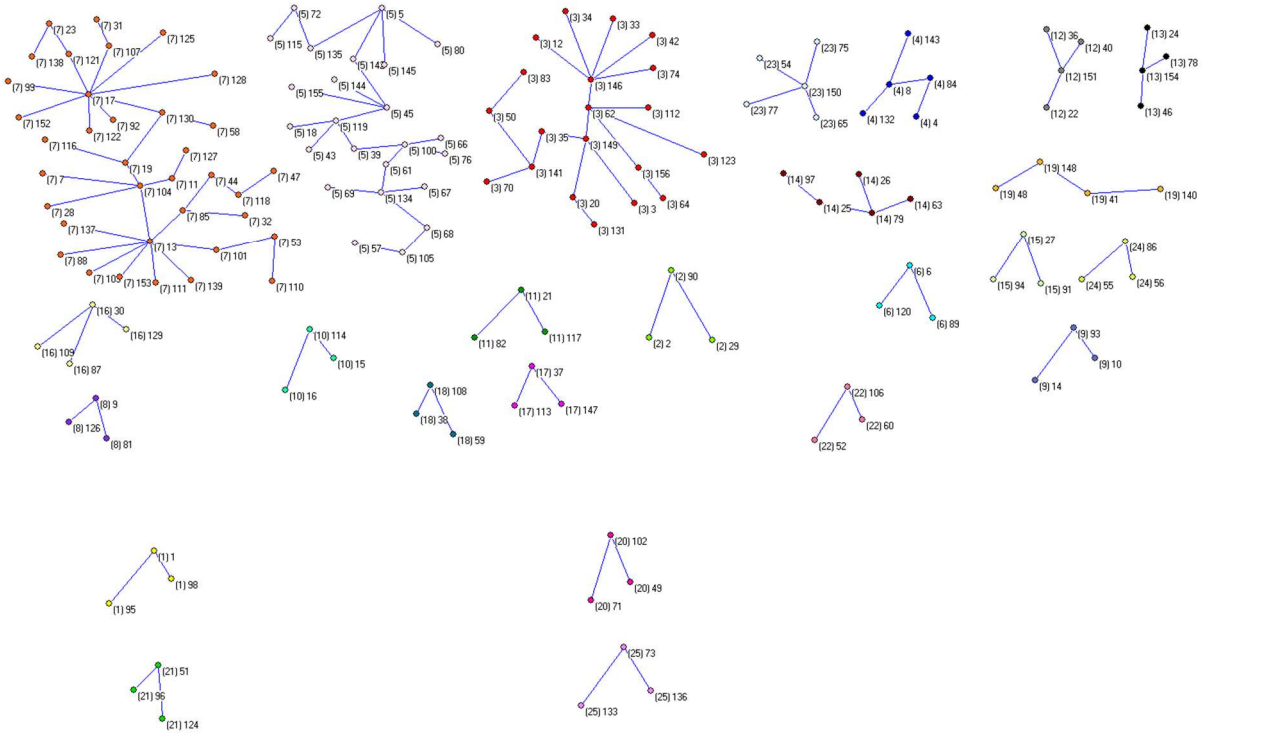


Figura 52. Isolados quatro componentes para análise

Figura 53. Apresentação de rótulos para cada nó

Cada rótulo presente na **Figura *53*** representa uma contratada ou uma organização pública. Dentre as 122 instituições encontradas destacam-se:

1. Nuclebras – Empresas Nucleares Brasileiras S/A;
2. Instituto de Pesquisa Econômica Aplicada (Ipea);
3. Instituto de Controle do Espaço Aéreo;
4. Empresa Brasileira de Pesquisa Agropecuária (Embrapa);
5. universidades em todo o Brasil;
6. Empresa Brasileira de Serviços Hospitalares;
7. Receita Federal do Brasil (RFB);
8. Banco Central (Bacen);
9. Casa da Moeda do Brasil;
10. Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama);
11. Polícia Rodoviária Federal;
12. Laboratório Nacional de Computação Científica;
13. Instituto Nacional de Tecnologia da Informação;
14. Fundação Oswaldo Cruz (Fiocruz);
15. Agência Nacional de Energia Elétrica (Aneel);
16. Agência Nacional de Águas (ANA;
17. Departamento Nacional de Infraestrutura de Transportes (Dnit);
18. Gabinete do Comandante da Marinha;
19. Estado-Maior das Forças Armadas;
20. Serviço Federal de Processamento de Dados (Serpro).
21. ..

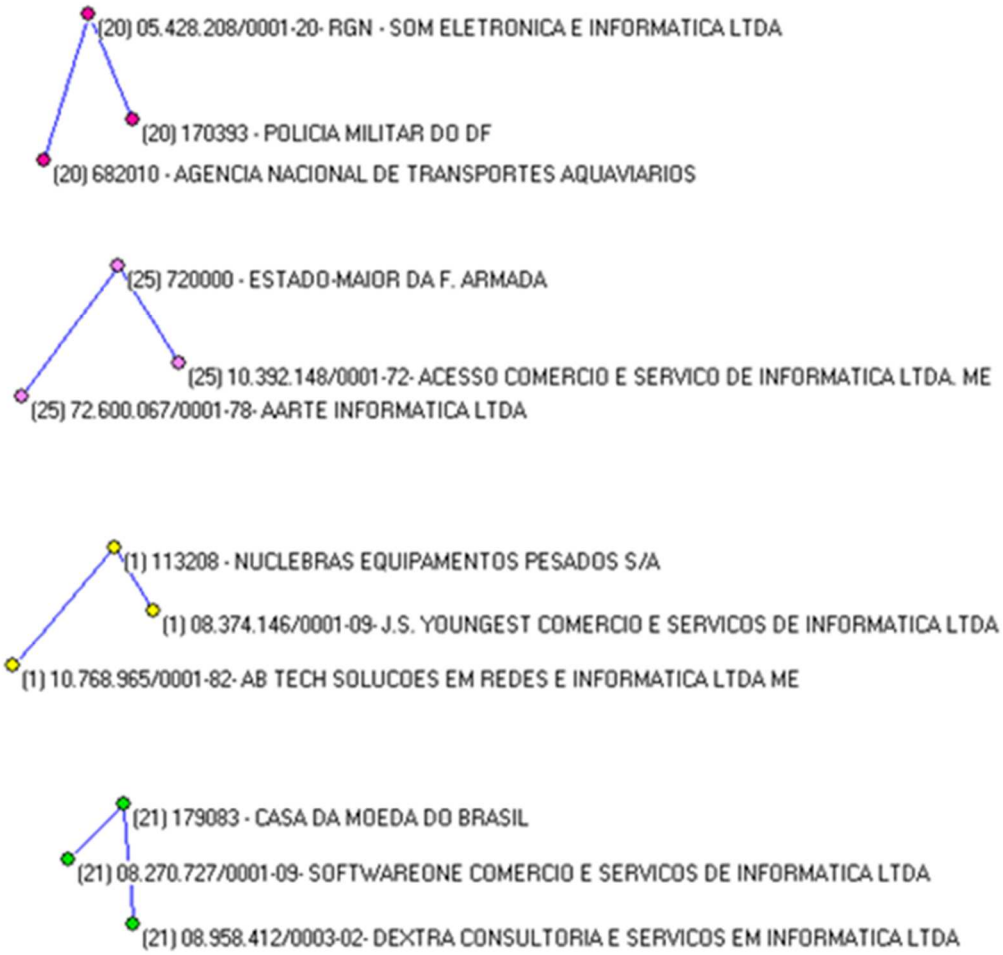


Figura 54. Recorte de quatro componentes para análise

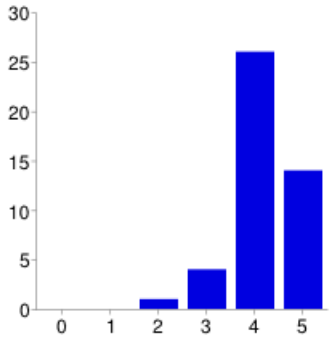
Os componentes da

Figura *54* apresentam a mesma topografia do caso estudado na primeira análise deste trabalho. Existem mais detalhes a serem realizados para se chegar a um ataque efetivo, mas é possível perceber a possibilidade e a facilidade de identificação de alvos após a construção deste método e o uso destas ferramentas. Na subseção 4.1.4 os dados serão mais bem discutidos.

4.1.3 Resultado da pesquisa de opinião

Seguem algumas estatísticas baseadas nos resultados das entrevistas. Serão apresentadas a pergunta e a estatística das respostas. As respostas foram de múltipla escolha e abertas. As respostas de múltipla escolha tinham uma escala de 0 a 5, onde 0 significa nada e 5 é o máximo.

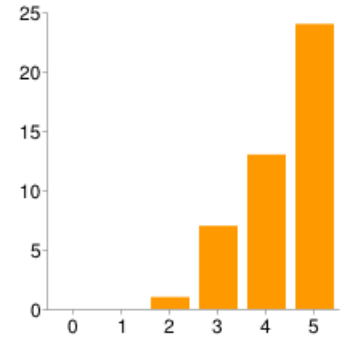
Como você considera sua prestatividade na sua unidade de trabalho?



0	**0**	0%
1	**0**	0%
2	**1**	2%
3	**4**	9%
4	**26**	58%
5	**14**	31%

Figura 55. Percentual sobre prestatividade própria

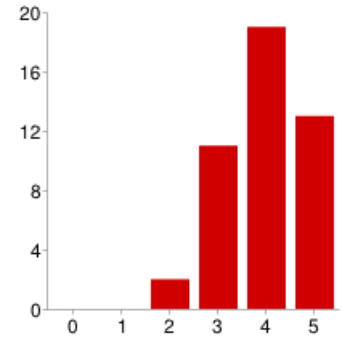
O quanto você considera a prestatividade importante para a eficiência das atividades laborais?



0	**0**	0%
1	**0**	0%
2	**1**	2%
3	**7**	16%
4	**13**	29%
5	**24**	53%

Figura 56. Percentual sobre a importância da prestatividade

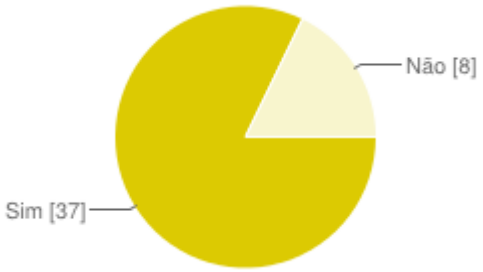
Quanto você considera sua prestatividade aos funcionários terceirizados na sua unidade de trabalho?



0	**0**	0%
1	**0**	0%
2	**2**	4%
3	**11**	24%
4	**19**	42%
5	**13**	29%

Figura 57. Percentual sobre prestatividade aos terceirizados

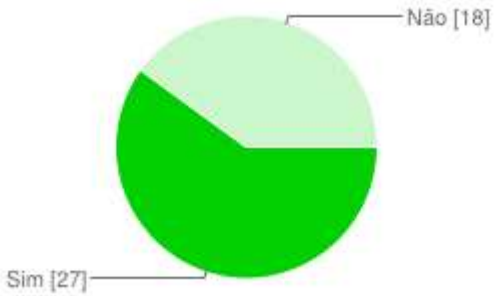
Seus superiores costumam delegar tarefas por telefone ou mensagem quando estão fora de sua unidade de trabalho?



Sim	**37**	82%
Não	**8**	18%

Figura 58. Percentual de delegação de tarefas remotamente

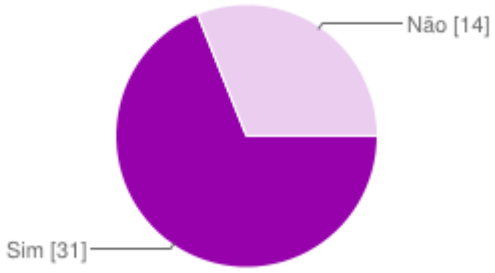
As empresas contratadas costumam receber informações para realizar suas tarefas fora de sua unidade de trabalho por telefone ou mensagem eletrônica?



Sim	**27**	60%
Não	**18**	40%

Figura 59. Percentural de tarefas executadas remotamente por terceiros

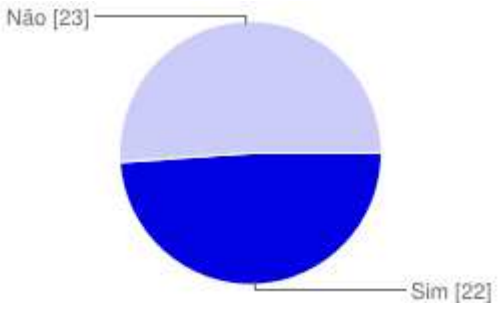
Já houve necessidade de acesso remoto aos equipamentos com os quais você costuma trabalhar?



Sim	**31**	69%
Não	**14**	31%

Figura 60. Percentual de pessoas que tiveram equipamentos acessados remotamente

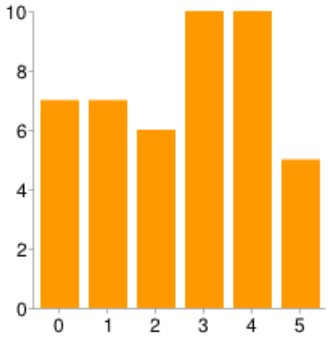
Todos os contratados que necessitam acessar os computadores que você trabalha são seus conhecidos?



Sim	**22**	49%
Não	**23**	51%

Figura 61. Percentual de pessoas que conhecem ou não quem acessa seus equipamentos remotamente

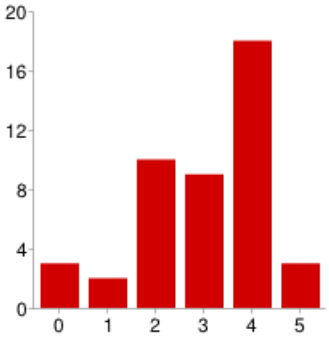
Com que frequência você trabalha com contratados/terceirizados por telefone ou mensagem eletrônica?



0	**7**	16%
1	**7**	16%
2	**6**	13%
3	**10**	22%
4	**10**	22%
5	**5**	11%

Figura 62. Percentual de trabalhos realizados remotamente

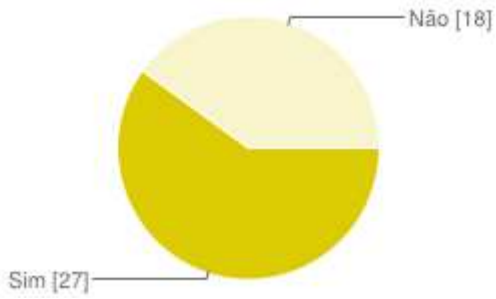
O quanto considera confiável seus contratados e/ou fornecedores?



0	**3**	7%
1	**2**	4%
2	**10**	22%
3	**9**	20%
4	**18**	40%
5	**3**	7%

Figura 63. Percentual de confiança nos fornecedores

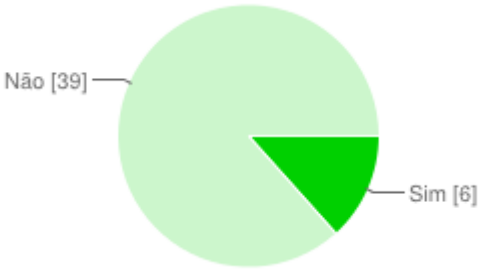
Você conhece algum caso de senhas serem enviadas por telefone ou mensagem eletrônica?



Sim	**27**	60%
Não	**18**	40%

Figura 64. Percentual de conhecimento sobre senhas enviadas por mensagem

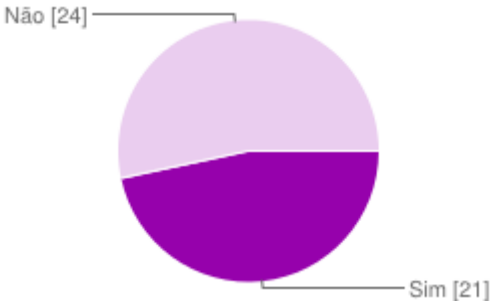
Você costuma receber listas de funcionários das contratadas periodicamente?



Sim	**6**	13%
Não	**39**	87%

Figura 65. Percentual dos que recebem ou não listas de funcionários prestadores de serviço

Há algum protocolo com o qual teve a oportunidade de trabalhar sobre procedimentos laborais com terceiros na sua unidade de trabalho?



Sim	**21**	47%
Não	**24**	53%

Figura 66. Percentual de pessoas que trabalham com protocolos laborais com terceiros

Você sabe o que é classificação da informação?

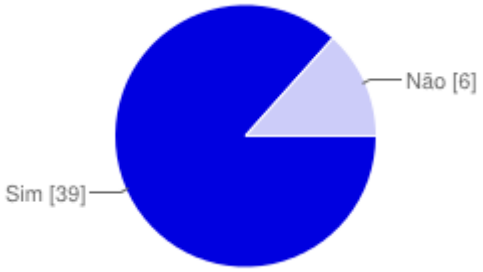
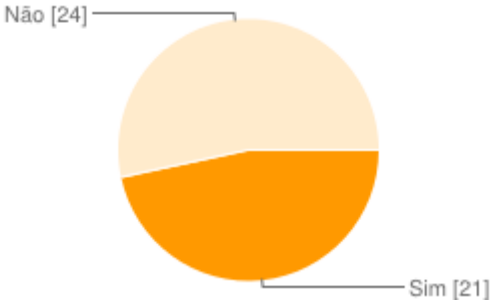


Figura 67. Percentual dos que conhecem ou não a classificação da informação

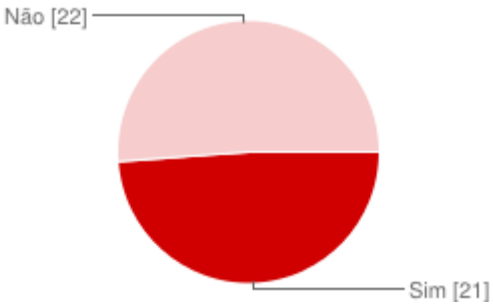
Você já classificou alguma informação onde trabalhou?



Sim	**21**	47%
Não	**24**	53%

Figura 68. Percentual dos que já classificaram informação

Você sabe o que é engenharia social e já teve algum curso corporativo sobre o tema?



Sim	**21**	47%
Não	**22**	49%

Figura 69. Percentual dos que conhecem ou não engenharia social

Vários consultados tiveram problemas com compras via internet, tendo os dados do cartão de crédito sido copiados provavelmente de outro *site* e utilizados em outra compra sem sua autorização, além disso, compraram produtos que nunca chegaram – preços atrativos demais são sempre motivo para desconfiança.

Um caso interessante para o estudo: um dos pesquisados teve sua senha de administrador do computador acessada; a vítima descobriu que esteve sendo observada por meses; quando notou tomou providências para eliminar essa situação, não relatou quais, mas pôde perceber que seus dados pessoais estavam sendo monitorados.

Um dos consultados sofreu um golpe por telefone celular: foi feita uma transferência para a conta bancária do bandido devido a uma promessa de prêmio. Outro pesquisado informou que uma vítima abriu seu *e-mail* e foi encaminhada a um *site* falso de banco. Um amigo de um dos consultados, através de um *site* de relacionamento, foi iludido por um homem e acabou enviando dinheiro para ele. A vítima, segundo o consultado, demonstrou certa inocência e pouca informação sobre tipos de golpes.

Houve um relato nas entrevistas de caso de *phishing*-scan envolvendo acesso bancário, executado por meio de *e-mail* falso. A pessoa, apesar de ser profissional de TI, disse que foi iludida em razão da semelhança da mensagem falsa com as mensagens do banco do qual era cliente, reportou que estava distraída na hora e só percebeu o golpe depois.

Uma vizinha de um dos consultados sofreu um crime por telefone: “O bandido ligou dizendo que tinha sequestrado seu filho, mas na verdade o filho dela estava viajando para Caldas Novas, a mãe, com medo, fez tudo o que o bandido pediu, inclusive depositando R$ 5 mil na conta do criminoso”. Ela relatou a experiência como terrível, desesperador, cruel e ficou indignada quando tomou consciência que tinha sido enganada.

Um colega de outro consultado sofreu uma tentativa de roubo de seus dados para acesso a *site* bancário. Foram utilizados *sites* falsos para essa ação, e ele descobriu bem rapidamente, acabou não tendo nenhum prejuízo. Outro consultado teve parentes que foram alvo de estelionatários tentando aplicar o golpe do sequestro falso por telefone, mas sem prejuízos também.

Relato de um dos consultados: “Enquanto estava trabalhando, uma senhora, colega de trabalho, recebeu ligação de um número não identificado informando que haviam sequestrado seu filho e pedindo resgate. Ela ficou muito nervosa, e um colega de trabalho assumiu a negociação. Enquanto tentava entender a situação e acalmar os bandidos, ele pediu que os demais colegas tentassem localizar o rapaz, supostamente sequestrado.

Felizmente conseguiram localizar o rapaz e descobrir que se tratava de um golpe para que a mulher transferisse dinheiro para os bandidos. Mas em vez de chamar a polícia, xingaram o bandido e desligaram o telefone".

Segundo um consultado, *sites* de recomendação sugerem outros *sites* que aplicam golpes. São apresentadas algumas ideias na Tabela 3, com opiniões dos consultados sobre fraudes, golpes e engenharia social, com informações mascaradas. As informações mascaradas são aquelas que não indicam diretamente nomes, fontes de informação e procuram preservar ao máximo os consultados e suas organizações. Cada linha da tabela é uma opinião de um consultado que foi destacada.

Tabela 3. Opiniões dos consultados, mascaradas

Opiniões sobre fraudes, golpes e engenharia social (mascaradas)
A internet é um campo minado para a proliferação e a perpetuação de golpes, fraudes e engenharia social. A facilidade proporcionada pela ausência do contato físico e a escala que um golpe pode atingir sem precisar levantar-se da cadeira fez com que os criminosos migrassem para esta plataforma. Uma boa parte dos golpes aplicados *online* são adaptações de métodos antigos, que geralmente se utilizam da ganância ou da curiosidade do usuário para conseguir sucesso. Outra parte se utiliza da engenharia social para coagir, amedrontar ou mesmo conquistar o alvo para o atingimento do objetivo. Portanto, a educação e a informação dos usuários ainda são mais eficazes do que ferramentas de proteção no combate às fraudes *online.*
Trabalhei em uma empresa na qual foi contratado um *software* para diagnosticar as possíveis falhas de segurança dessa natureza. Além disso, foi instituída na empresa toda uma normatização de segurança da informação, assim como a classificação da informação.
Informações sigilosas devem ser passadas estritamente a quem de direito e, dependendo da classificação do sigilo, evita-se usar qualquer meio eletrônico. Sobre fraudes, sempre buscar referências de quem já teve êxito em determinada ação no ambiente virtual e, se possível, de quem não teve para saber o porquê.
Na organização em que trabalho, os empregados são capacitados anualmente sobre segurança da informação, onde recebemos esclarecimentos sobre esses tópicos, entre outros. Afinal, o "elo mais fraco" em segurança da informação é o fator humano. Sempre procuro aplicar as boas práticas de segurança da informação, evitando hábitos que possam causar transtornos e situações embaraçosas.
Minha experiência é teórica e dentro do governo federal. Sei que o governo federal classifica as informações segundo seu grau de sigilo e relevância. Eu nunca cheguei a classificar

nenhuma informação. Quando trabalhei em um tribunal estadual, participei da elaboração das rotinas sobre tratamento de processos que estão em segredo de Justiça. O fluxo desse tipo de processo é bastante rigoroso, e sua disponibilidade é extremamente restrita. Quanto a fraudes e golpes por meio de engenharia social, não experimentei ou vi um caso.
Na instituição onde trabalho preciso dar muita atenção à classificação da informação, pois trabalho como gerente de configuração e mudança, e cada artefato armazenado no repositório tem seu nível de classificação a ser observado.
Particularmente evito fazer transações via internet porque não confio muito, já ouvi várias histórias de golpes e fraudes. Já recebi *e-mails* de fontes aparentemente confiáveis (tentando se passar por algum conhecido) solicitando dados pessoais.
Classificação da informação: conjunto de ações referente a níveis e critérios de proteção das informações garantindo a confidencialidade. Engenharia social é a habilidade da ação humana de obtenção de dados reservados.
Temos uma política de segurança da informação na organização em que trabalho. Com a orientação adequada, reduzem-se riscos de ser vítima de fraudes. Isso é uma questão cultural que deve ser intensamente apoiada por ferramentas educacionais, pois a maioria das pessoas não quer gastar o tempo em seguir regras de segurança, tanto físicas como lógicas, para sua proteção. A minha experiência diz que o problema acontece naqueles momentos de distração ou de extrema pressa, quando a pessoa não percebe a fraude. Se a pessoa estiver condicionada a perceber as fraudes eletrônicas, conhecer os tipos de engenharia social para obtenção de segredos pessoais e ter uma noção de classificação da informação, o fato da obtenção ilícita do dado ou informação se torna mais difícil.
Classificação da informação: muito difícil classificar certos tipos de casos. Fraudes, golpes e engenharia social na internet: necessita muita atenção das pessoas e disseminação do conhecimento de fraudes realizadas pelo crime organizado. Classificação da informação: conjunto de ações referente a níveis e critérios de proteção das informações garantindo a confidencialidade.

Na subseção 4.1.4 os dados serão mais bem discutidos.

4.1.4 Discussão

Finalmente se chegou ao ponto em que se podem cruzar os cenários hipotéticos estudados com informações reais extraídas do Portal da Transparência a fim de demonstrar as possibilidades da análise de redes sociais para a engenharia social. Esse inter-

relacionamento conceitual criado entre informação, confiança, risco, segurança da informação e a análise de redes sociais e a engenharia social permite apresentar possíveis explorações de vulnerabilidades em cenários de ataques hipotéticos.

Aqui serão utilizados os cenários hipotéticos de engenharia social, os dados coletados por meio da aplicação de questionários e o cruzamento com casos reais extraídos do Portal da Transparência. Esses casos são mais bem visualizados com sua transformação em sociogramas.

Por que trabalhar com cenários hipotéticos? Realizar teste de segurança da informação e comunicações (SIC) em um ambiente real é um problema inerente ao tema SIC. Para realizar um ataque é necessário agir agressivamente sobre um alvo e efetuar uma quebra de segurança. Na maioria dos casos, um ataque tem algum resultado negativo. A menos que haja uma autorização expressa, como é o caso dos testes de intrusão, é óbvio que não é recomendado realizar um teste de ataque em SIC à revelia. Provavelmente por isso foram encontradas tantas discussões em SIC utilizando-se cenários hipotéticos.

Tanto em obras literárias sobre testes de intrusão quanto em livros a respeito de ataques reais no campo da segurança da informação a identificação do alvo é um processo sistemático e a primeira etapa do ataque. Sabendo que diversos autores presentes nesta dissertação – Mitnick e Simon, Watson et al., Hadnagy, Allen etc. – trabalham os conceitos e exercitam seus ataques de SIC em cenários, decidiu-se utilizar os cenários dessas doutrinas.

Alguns autores apresentados explicam a identificação do alvo utilizando a varredura de vulnerabilidades, que é a busca sistemática de informações de vulnerabilidade de alvos, fraquezas. Outros autores chamam de *footprinting* – a fina arte de levantar informações do alvo –, em que se coleta o máximo de informações sobre a segurança de um alvo, seja ele uma pessoa, seja uma organização ou outro ator social.

Conforme verificado, analistas tipicamente analisam os dados de uma rede social em uma ou duas perspectivas: (1) relacional ou (2) abordagem posicional. Após a aplicação das transformações, das extrações e das classificações da rede, com uma abordagem relacional e posicional, os papéis de corretagem e mediação ficam latentes. Pode-se afirmar, com base em tudo o que foi exposto neste trabalho, que os papéis de corretagem da ARS podem ser explorados com a engenharia social.

Observe-se o caso da **Figura *70***, em que o Estado-Maior das Forças Armadas tem contratos com duas empresas de um mesmo contexto – contratações de tecnologia da informação. Nesse caso, o engenheiro social poderia, por *e-mail* ou telefone, iniciar uma

relação com a empresa Acesso Comércio e Serviço de Informática Ltda. e com a empresa AArte Informática Ltda. Essa relação, à medida que fosse aprofundada, estabeleceria confiança por meio da comunicação, então poderia disponibilizar ao engenheiro social informação sobre os jargões das empresas e das práticas de trabalho. Essa relação poderia ser estabelecida de tal forma que o atacante poderia identificar vulnerabilidades nas relações entre as empresas e o Estado-Maior das Forças Armadas.

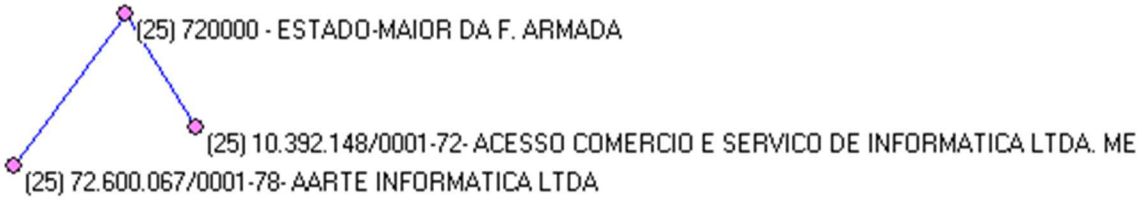


Figura 70. Tríade Estado-Maior e contratadas

Melhor exemplificando: imagine-se Didi Sands, do caso apresentado à página 88, procurando informações sobre servidores públicos no Estado-Maior das Forças Armadas. Provavelmente Didi Sands sabe que o nível de segurança dessa instituição é mais elevado que o das empresas Acesso Comércio e Serviço de Informática Ltda. e AArte Informática Ltda. Portando, ela iria realizar um ataque primeiro nas duas empresas e utilizar essas informações para penetrar no perímetro de informação que ela deseja dentro do Estado-Maior.

Provavelmente a Casa da Moeda, **Figura *71***, tem a mesma relação com as empresas Software One Comércio e Serviços de Informática Ltda. e Dexta Consultoria e Serviços em Informática Ltda. que a estudada no caso anterior do Estado-Maior das Forças Armadas.

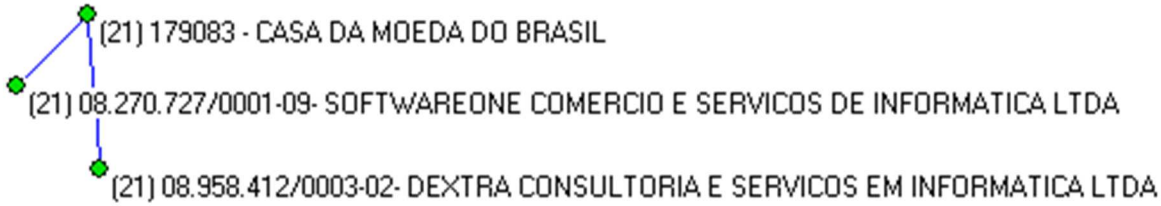


Figura 71. Tríade Casa da Moeda e contratadas

Existe um *informational link* entre a Acesso Comércio e Serviço de Informática Ltda. e a empresa AArte Informática Ltda. Outro *informational link* entre a Software One Comércio e Serviços de Informática Ltda. e a Dexta Consultoria e Serviços em Informática Ltda. Nos cenários apresentados nas **Figura *70*** e **Figura *71***, ora um ator é emissor ora é receptor da comunicação. Nessa situação o engenheiro social pode, maliciosamente, assumir o papel

de mediador da comunicação.

O mediador da comunicação pode assumir qualquer dos papéis de mediação apresentados na **Figura *31***. Quando o engenheiro social assume o papel de coordenador nos casos apresentados anteriormente ele se passa pela Casa da Moeda ou pelo Estado-Maior. Dessa forma, poderia abusar da confiança das outras partes no relacionamento por meio de persuasão e falsa autoridade.

Na exploração da vulnerabilidade com o papel corretor itinerante, poderia barganhar informações em uma falsa promessa de vantagem às outras partes. Por exemplo, solicitando informações de outros setores e deixando a entender que isso fortaleceria a relação comercial.

O papel de ligador ou conector poderia ser utilizado para se obter informação da segunda empresa a fim de atacá-la com a estratégia de realizar uma ataque mais preciso ao alvo principal em uma segunda oportunidade – uma falsa mediação entre membros das diferentes empresas. Como pode ser notado, o uso de papéis da ARS pode ser uma estratégia de ataque pós-seleção do alvo. Portanto, seria possível utilizar a análise de redes sociais para realizar ataques de engenharia social.

Como um aspecto agravante, baseado na pesquisa, a prestatividade é considerada essencial para a execução das atividades laborais, principalmente de governo. A publicidade das ações é princípio da administração pública, o que preocupou alguns dos consultados e reforça a criticidade do cenário público brasileiro quanto à engenharia social, pois, em momentos de pressa, boa-fé e distração os golpes acontecem.

Deve-se destacar que os consultados na pesquisa de opinião, apesar de conhecerem pessoas que sofreram algum tipo de golpe, ou eles mesmos, apresentaram conhecimentos sobre o tema de maneira prática, o que é muito interessante e nos remete ao que Schneier apresentou: a sociedade sempre pensa que é melhor em detectar esse tipo de situação do que na verdade é. Os consultados consideram-se conhecedores do assunto, mas não descartam a necessidade de treinamentos e não se consideram fora de ameaça. O cenário é crítico:

- 82% dos consultados recebem ou enviam tarefas por *e-mail*, possibilitando o uso deste canal para ataques de engenharia social, por exemplo, com a personificação;
- 69% já tiveram seu computador acessado remotamente, e mais da metade não conhecia quem se identificou que iria fazer o acesso remoto;
- 60% presenciaram envio de informações restritas por *e-mail*, por exemplo, senhas

de acesso.

Outra informação interessante que merece destaque é que não foram identificados norma, protocolo ou fiscalização que reprimam certas atividades da engenharia social, mesmo no contexto das informações de cunho pessoal e íntimo. Não há regulação para a coleta de dados na internet. A facilidade de obtenção dos dados é uma vantagem quando se utilizam dados abertos. Eles são livres para uso, e qualquer um pode utilizá-los, inclusive os elementos mal-intencionados.

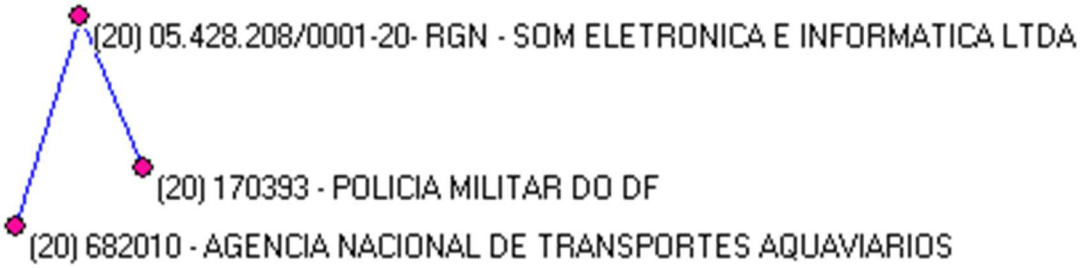


Figura 72. Tríade PMDF e Antaq

No caso apresentado na Figura 72, poderiam ser utilizados os outros papéis da corretagem mal-intencionada, da mediação maliciosa das comunicações. A Polícia Militar do Distrito Federal (PMDF) e a Agência Nacional de Transportes Aquaviários (Antaq) estão formando um *Informational Link* por meio da empresa Som Eletrônica e Informática Ltda.

O mediador atuaria como um representante de uma das organizações, após uma investidada sobre a empresa contratada. A regulagem do fluxo de informações poderia ocorrer caso um ataque à empresa contratada desse ao engenheiro social o controle sobre algum canal de comunicação entre as partes. Por exemplo, algum representante comercial poderia ser personificado[25] e, dessa forma, haveria abertura para colher informações sensíveis.

O papel de porteiro também poderia ser utilizado para regular algum fluxo de informações para os órgãos. Utilizando-se o nome de algumas das organizações poderia ser mais fácil a investida sobre algum ponto de falha específico. Ainda em uma abordagem proposicional, podem-se utilizar as ideias de Lewicki e Bucker e suas três dimensões distintas da confiança, em que quanto mais conhecemos um indivíduo e suas intenções,

[25] Personificação ocorre quanto um atacante pode introduzir ou substituir uma identidade induzindo outros a pensarem que esta identidade falsa, ao invés da legítima, é a correta. Dessa forma, o atacante se passa por outro indivíduo.

mais confiamos nele.

É claro que o ataque de engenharia social não é executado do dia para a noite. Mas se pode observar que com a repetição de padrões das relações sociais há possibilidade de exploração de vulnerabilidades. Dessa forma, as respostas dos questionários indicam que o cenário atual da administração pública é propício para os tipos de ataques discutidos nesta dissertação. Além disso, os padrões de cenário se repetiram nos casos reais coletados na internet, discutidos anteriormente.

Uma das vantagens da análise de redes sociais é a facilidade com que se trabalha com uma grande quantidade de dados e com que se manipulam esses dados, obtendo-se resultados de simples interpretação. Se o atacante utiliza técnicas *ad-hoc* de identificação de alvo, provavelmente terá de gastar muita energia para chegar ao mesmo resultado de identificação de alvos que o conquistado com a análise sistemática de redes sociais. Portanto, um benefício dessa análise para a defesa seria utilizar essas técnicas de análise para prever possíveis vulnerabilidades e algumas ações maliciosas na intenção de evitá-las.

Nos casos discutidos neste trabalho, com o método de identificação de alvos o ataque hipotético não possuía automatização. Porém, acredita-se que é possível um ataque automatizado em massa enviando-se *e-mail* com *fishing-scan* com base em informações coletadas da web, baseando-se no perfil dos alvos e em sua posição na rede social, selecionando-se o tipo de exploração de vulnerabilidades de uma ferramenta, por exemplo, o SET.

Imagine-se todas as tríades presentes na **Figura *52*** sendo consultadas automaticamente, isso provavelmente aumenta o poder de seleção do alvo. A automatização seria um benefício para o ataque, e incrementada com o uso da inteligência pode gerar proporções grandiosas.

Conforme exposto nesta dissertação, uma rede social pode ser decomposta em várias tríades. Portanto, seria possível imaginar várias tríades em uma rede social formada pelo componente 7 da **Figura *52*** – o componente vermelho no canto superior esquerdo. Uma extração desse componente pode ser observada na **Figura *75***.

Curiosamente, em sua quase totalidade o componente é formado por universidades ou instituições de ensino quando se está observando as instituições públicas. Mas o que merece destaque são as possibilidades de exploração utilizando-se as tríades da mesma forma, como foi exposto antes. Claro que se trata de um caso mais complexo, e ele não será analisado por uma questão de extrapolação de propósitos.

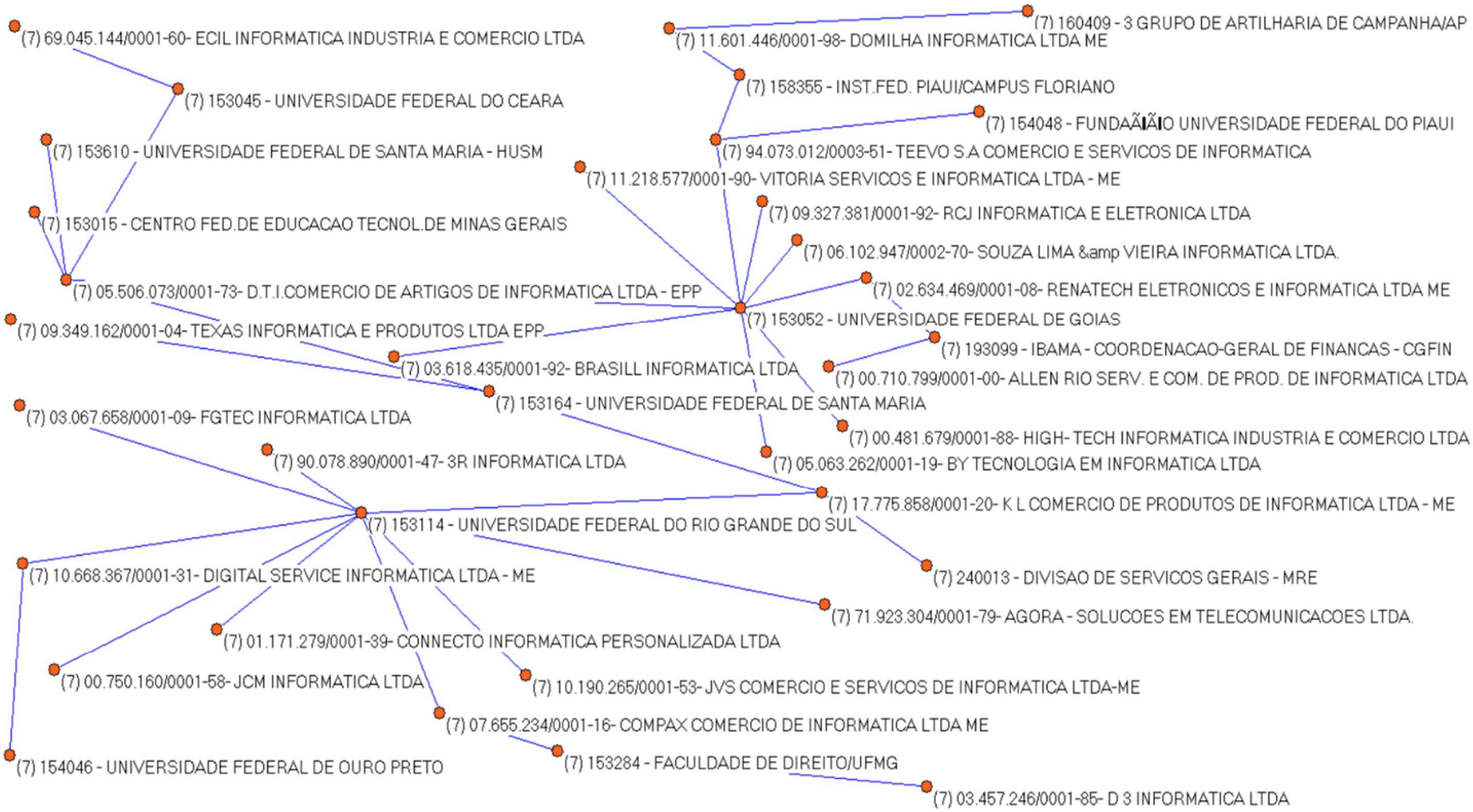


Figura 73. Componente com universidades

Provavelmente já estão sendo usados métodos de automatização de ataques como este na internet. Os *bad guys* não medem esforços! O *hacker* é o sujeito que quebra as regras que julga estúpidas para conseguir ganhos que ele considera mais inteligentes. Deve-se lembrar de que a maioria dos consultados teve seus dados pessoais roubados ou estes foram manipulados por meio de ataques de engenharia social pela internet.

Não se identificou a necessidade de os dados serem estruturados para serem considerados dados abertos. O fato de os dados não serem estruturados aumenta a complexidade da coleta e da análise. Encontrou-se em outras fontes definição de dados abertos como uma fonte de dados estruturados. Um memorando, bastante citado na internet, do presidente dos EUA, Barack Obama, diz: “Dados abertos: para efeitos do presente memorando, o termo ‘dados abertos’ refere-se aos dados estruturados disponíveis publicamente de uma forma que permite que esses dados sejam totalmente acessíveis e utilizáveis por usuários finais (tradução do autor)” (CREATIVE COMMONS, 2013).

Vê-se com esse método de ARS para identificação de alvos a possibilidade e o benefício de serem observados pontos frágeis, vulnerabilidades e ameaças nas redes de relacionamentos entre fornecedores, contratantes, fabricantes e outros atores sociais no contexto das TIC. O uso do método de ARS para identificação de alvos possibilitaria a detecção de pontos frágeis, vulnerabilidades e ameaças. Haveria o fornecimento de informações para análise da segurança de informações do Estado brasileiro, possibilitando uma melhor gestão de riscos.

É sabido que a informação é o objeto a ser protegido na segurança da informação. O foco primordial da SI é a garantia da manutenção dos três aspectos fundamentais da informação: confidencialidade – propriedade de a informação ser acessada por quem tiver autorização e de não ser acessada por aqueles que não a tiverem; integridade – propriedade de a informação não ter sido alterada por qualquer agente desautorizado; disponibilidade – aspecto da segurança que garante a disponibilidade da informação a todos os autorizados sempre que dela necessitarem.

Observando-se que a autorização está presente nas três características básicas da segurança da informação (**Figura *74***), pode-se propor: se **A => C**, então **C** é ponto fundamental em SIC, ou seja, sendo **C** a Confiança e **A** a Autorização, pode-se estabelecer que autorização implica confiança, pois acredita-se que autorizamos quem confiamos. Como não é possível prever todas as ações de qualquer autorizado, conclui-ser que sempre haverá confiança nas autorizações.

Logo, **C** é parte do cerne da segurança da informação, pois há risco latente na autorização, que é a transferência do poder agir ao indivíduo que recebeu a confiança de acesso ou escrita a alguma informação. Conforme visto nesta dissertação, confiança implica risco, e a querela da segurança da informação é a gestão de riscos.

O ponto principal no processo decisório da segurança da informação é decidir como serão tratados os riscos levantados. Portanto, se a administração dos riscos, ou seja, seu controle, é efetiva, fundamentalmente a gestão de riscos será efetiva bem como a SIC.

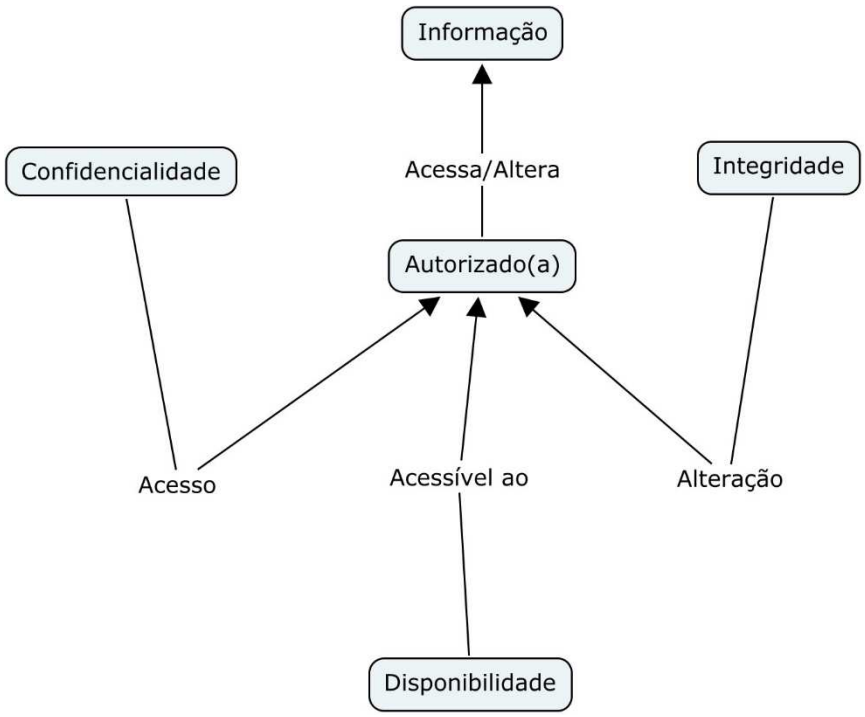


Figura 74. Relação entre autorização, informação e propriedades básicas da segurança da informação

Os ataques persistentes avançados (APA) são responsáveis por uma aguda preocupação. As ideias de Lewicki e Bucker podem esclarecer por que o APA é mais avançado que os ataques que utilizam regras bem definidas. Observa-se que o nível CBT seria a confiança baseada no entendimento da recompensa e punição bem definidas. Quando há um ataque em nível de vulnerabilidade de máquina a confiança CBT é quebrada.

Os aspectos KBT e IBT são a confiança nos termos da previsão e da dependência e fundamentada na internalização e no entendimento das intenções e dos desejos do outro. Aqui há APA, pois o aspecto persistente do ataque explora a confiança construída pouco a pouco. No caso de KBT e IBT, a comunicação interpessoal pode ser a chave do ataque.

Dessa forma, quanto maior o aprofundamento das relações, provavelmente maior será o nível de confiança interpessoal.

Se fosse possível formalizar o exposto anteriormente, poder-se-ia dizer que a confiança é uma relação proporcional entre o risco, uma função modificadora baseada no conhecimento aprofundado, e uma regulação, que traria como cursor de compasso as informações de contexto, como pode ser visto na Figura 75.

Figura 75. Relação entre autorização e confiança

É preciso compreender o fluxo informacional, o conteúdo, os usuários e o contexto no espaço para identificar os possíveis alvos dos ataques à segurança da informação, principalmente no caso específico estudado nesta pesquisa. A percepção humana das informações contextualizadas faz toda a diferença de quais níveis de proteção cada informação deve possuir. Assim, com esses elementos poder-se-á mediar a comunicação da informação buscando a segurança da informação adequada.

Por fim, pode-se afirmar, em um “mar” de informações, que o uso desse método e dessas ferramentas pode promover a identificação de alvos de forma mais objetiva e sistemática, sendo facilmente automatizada. O poder de um ataque que atinge seus objetivos é a combinação de técnicas e ferramentas.

É claro que este método não esgota o assunto. Mas essa linha de pensamento abre a discussão sobre riscos, problema para o qual não foi identificado qualquer tratamento na

administração pública. Após o exposto, parece viável e efetivo o uso da ARS como ferramenta de segurança. Se protocolos e procedimentos preestabelecidos tivessem sido seguidos nos ataques vividos pelos consultados talvez os crimes não tivessem acontecido.

4.2 Conclusão

Depois da exposição do arcabouço teórico deste trabalho a respeito do que é a CI, a comunicação e a mediação, conclui-se que a informação pode ser o padrão de organização dos objetos – dados – no espaço, no “mundo” de um sujeito, seja em um modelo mental seja em um espaço físico. Ela pode ser o objeto que flui em uma comunicação. Ela pode ser o produto da organização dos dados para gerar conhecimento. A informação é percebida por um sujeito por meio da observação da disposição dos objetos presentes em um contexto.

Sob outro ponto de vista, informação, dado e conhecimento são conceitos muito interligados. Definir informação sem tratar dos demais conceitos é muito difícil. Porém, é certo que informação não é dado nem conhecimento. Pode-se definir informação simplesmente descrevendo suas partes. Informação é algo *prima facie*, por exemplo, assim como se poderia definir carro como sendo um automóvel.

A resposta à pergunta “o que é um carro?”, pode ser “um carro é um carro!”. Não há necessidade de provas para se definir um carro, à primeira vista é óbvio. Mas para uma definição mais exata pode ser necessário descrever o que vem a ser um carro, por exemplo – um carro tem quatro rodas, um compartimento para o motorista e os passageiros, é motorizado, etc.

É possível definir algo descrevendo-o ou descrevendo o que ele não é, por exemplo: se há três rodas, não é um carro, se há duas rodas, idem. Nessa esteira, pode-se definir informação descrevendo-a, logo, são necessários outros conceitos: dado e conhecimento, assim como o conceito de roda e motor foi preciso para definir o que é um carro.

Como foi visto, para entender o que é informação é importante entender o processo de comunicação. Ao compreender tal processo acredita-se que a manifestação, a forma, o contexto e o significado da informação podem ser percebidos com mais clareza. O fluxo da informação pode ser entendido e analisado com o uso de modelos, desde os modelos lineares até os modelos de comunicação em rede.

Considerando o que Borko defende, a CI investiga as propriedades, o comportamento da informação e as forças que governam o fluxo da informação. Os controles de segurança da informação e da comunicação são elementos apoiadores da mediação da informação, seja em momentos de cooperação seja em momentos de trapaça, como doutrinou Schneier.

Assim, a comunicação e a mediação são objeto de análise da SI, e esta é objeto de

estudo da CI. Pode-se dizer que a mediação da comunicação seria o estudo dos meios midiáticos e de intermediação humana – *gatekeepers* – para a realização da comunicação e da informação. A mediação estende a comunicação humana e o processamento da informação.

A semelhança conceitual entre o modelo de comunicação e mediação de Baker, o *Informational Link* de Dretske, conceitos de homofilia e as teorias de sociogramas levam à afirmação de que cabe o uso da ARS nos estudos de comunicação, confiança e segurança da informação. A comunicação informal de Baker é representada por um grafo, e sua *Informational Link* e sua comunicação formal são representados por um sociograma em estrutura de árvore.

Nessa linha, a CI é uma disciplina que investiga as propriedades e o comportamento da informação bem como as forças que governam seu fluxo. Por sua vez, a ARS pode ser utilizada para identificar e analisar, nas organizações e nas empresas, os fluxos de informações. Os profissionais da segurança da informação da atualidade devem estar ligados à ciência da informação a fim de aprimorar seus conhecimentos em ARS, como Fernandes (2010d) afiançou.

Na conjuntura deste estudo, a confiança foi observada como um fenômeno social. Como dito, as informações de uma organização estão inseridas em um contexto, possuem um conteúdo e usuários. Além disso, a confiança é também sensível ao contexto. A confiança pode ser estudada por meio da ARS, conforme Everton (2013). Entende-se que a confiança pode manifestar-se no cenário do fluxo da informação, indo ao encontro de tudo o que foi apresentado, porque a confiança é desenvolvida com base nas comunicações, e a comunicação organizacional, por sua vez, é formada pelo fluxo de mensagens em uma rede de relacionamentos interdependentes, conforme defende Baker. As mensagens trocadas no ambiente organizacional são formais e informais. A estrutura da comunicação formal funciona por intermédio de regras, regulações, processos e é caracterizada por mais de um canal formal de comunicação. A estrutura informal de comunicação é criada entre as pessoas em qualquer canal e direção e emerge do relacionamento interpessoal. Os dois tipos de comunicação se completam e são necessários para o bom funcionamento de uma organização. No contexto mundial atual, as mudanças tecnológicas, inclusive a internet, têm levado a um cenário caótico e complexo na seara da informação organizacional.

Desse modo, a ARS estuda o fluxo de informações e relacionamentos interpessoais, podendo-se concluir que ela pode ser usada para pesquisar o fenômeno da confiança. Então, nas organizações existe um espaço de comunicação, e nele se encontram

relacionamentos expressos e interdependentes, dotados de manifestações de confiança. A análise de redes sociais pode auxiliar nas ponderações desse cenário por meio da observação das comunicações, favorecendo a modelagem da confiança entre as partes e a exposição dos riscos aos quais estas estão expostas.

Por fim, a confiança está presente nas comunicações e pode ser percebida por meio das proposições matemáticas e medida com o uso da observação. Precisar a quantidade de confiança e os riscos a ela relacionados ainda é um desafio, bem como o quanto é arriscada a exposição de alguém a uma situação insegura de confiança.

Portanto, entender o fluxo informacional para construir os mecanismos de segurança da informação e os modelos de comportamento obrigatório é uma forma de fortalecer os mecanismos de pressões institucional e social. Apesar de existir confiança em qualquer relação institucional, as coerções expressas em um contrato, por exemplo, fortalecem a confiança entre as partes.

Muitas vezes os acordos sociais são estabelecidos de forma remota por meio de um sistema de informação, diferentemente do que ocorria em tempos passados, quando a presença física era indispensável para a efetivação desses acordos. Os acordos remotos podem facilitar o abuso da confiança por meio da personificação, por exemplo. Esse abuso pode ser a causa do fracasso de projetos organizacionais, ou mesmo do malogro da organização, devido à violação das propriedades básicas da segurança da informação.

A busca de novas soluções para problemas cotidianos de segurança da informação deve ser constante. As premissas utilizadas no passado para a SI provavelmente são as mesmas hoje, porém é necessário pensar na perspectiva e no contexto informacional atual, inclusive pensar nas consequências sociais, na velocidade de tráfego da informação, na escala, no descontrole, etc.

A análise de redes sociais traz aspectos objetivos para se identificar estruturas sociais por meio da observação da realidade. A ARS é a nova inteligência necessária para os assuntos de segurança, como afirmou Ressler. Contudo, como defendeu Turner, o uso extensivo da matemática e de algoritmos de computador excede em muito as habilidades técnicas da maioria dos cientistas sociais. Desse modo, é óbvio se utilizar a CI para pesquisar o fenômeno da segurança.

Deve-se lembrar que Everton defende que a ARS pode estudar a condução e a difusão de vários tipos de benesses materiais e não materiais na rede social, entre elas informações e confiança. Então, esse arcabouço conceitual é o fundamento para se concluir que a ARS pode ser usada na mediação da informação no contexto da segurança da

informação.

O mais importante do uso e da aplicação de técnicas quantitativas é a possibilidade de visão holística. Mas é essencial o desenvolvimento tanto de pesquisas quantitativas, com base tecnológica, que contribuam para uma percepção mais exata da realidade, como de técnicas qualitativas, sabendo que é inexorável sua contribuição no aspecto humano da pesquisa.

Esta pesquisa pretendeu encontrar alguns aspectos objetivos nas relações de confiança e riscos no contexto da segurança da informação. Para tanto, procurou-se responder à pergunta de como podem ser identificados alvos para ataques de engenharia social no que se refere ao abuso da confiança, utilizando como ferramenta a análise de redes sociais aplicada em dados abertos da administração pública.

O objetivo geral da pesquisa foi identificar alvos para a engenharia social, utilizando para isso o método de análise de redes sociais na disciplina segurança da informação, tendo as redes sociais usadas sido obtidas em fontes de dados abertos da administração pública. Esta pesquisa é classificada em aplicada qualitativa diacrônica descritiva, e suas técnicas de coleta e análise de dados são o estudo de caso e a análise de redes sociais. Trata-se de uma pesquisa quase experimental, pois, apesar de incluir testes e experimentos, o pesquisador não teve o controle total sobre o ambiente.

Para se chegar ao objetivo principal foram traçados alguns objetivos específicos. No referencial teórico foi possível conectar conceitualmente a ciência da informação, a segurança da informação, a engenharia social, a confiança e a análise de redes sociais. Pode-se observar na **Figura *76*** um resumo, em forma de mapa conceitual, do que se conectou conceitualmente. Trata-se de um modelo que tenta apresentar uma visão global dos conceitos mais importantes abordados no referencial teórico. Acredita-se que é possível perceber a relação, principalmente, entre informação, confiança, risco, segurança da informação e a análise de redes sociais sobre a engenharia social.

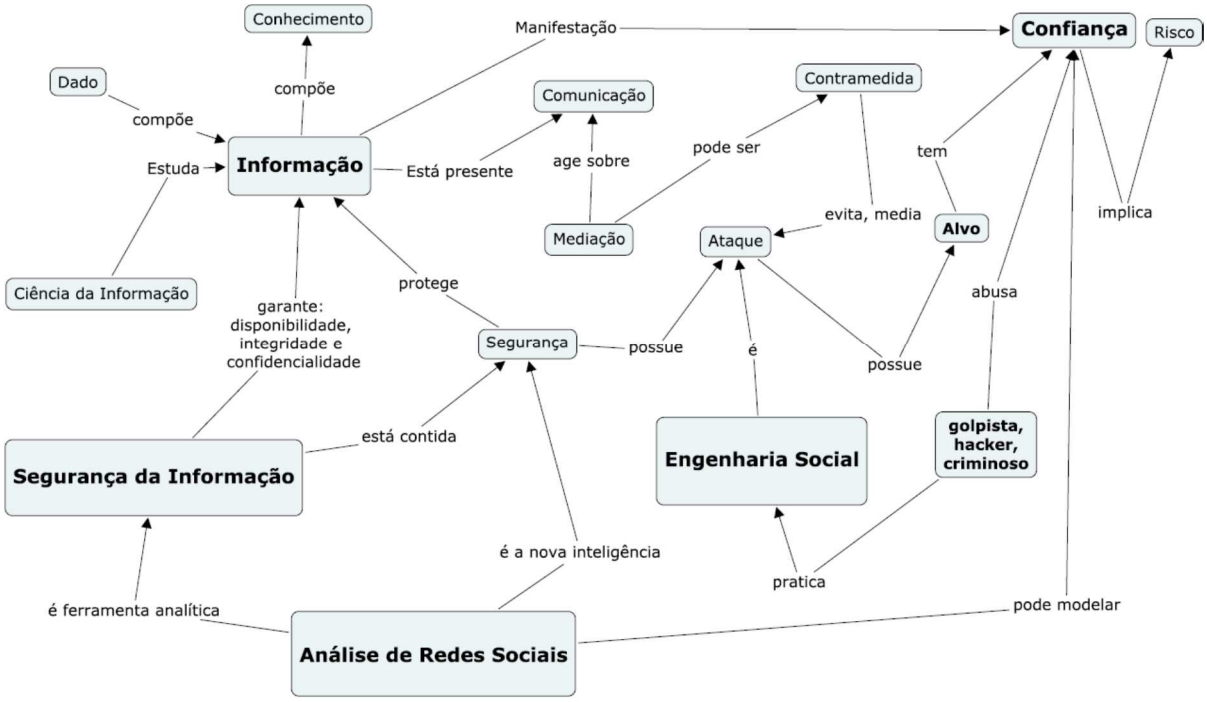


Figura 76. Mapa conceitual do referencial teórico

A conclusão quanto aos modelos de comportamento obrigatório e confiança foi superficial. Por exemplo, a gramática seria um modelo de comportamento obrigatório na comunicação, e todos aqueles que a utilizam, quando a utilizam, confiam que o receptor da mensagem também a conhece. Imagine-se o risco em uma situação de pouso e decolagem de um avião, com diversas vidas dependendo dos pilotos. Todos na aeronave confiam que os pilotos saberão comunicar-se com a torre. Para isso, o entendimento da linguagem e da comunicação é fundamental. Se o piloto ou o copiloto não souberem as regras de comunicação com os agentes na torre de controle dos aeroportos um acidente é muito provável.

Entende-se aqui que o processo de gestão da segurança da informação se inicia basicamente com um levantamento ou a análise de qual informação se quer proteger e quais os riscos associados. O processo segue com a seleção e a implantação de controles de segurança da informação para tratar, mitigar ou contornar os riscos que não puderam ser eliminados, aceitos ou transferidos. A gestão da segurança da informação acompanha os controles e as contramedidas de segurança da informação e realiza ajustes neles ou no processo caso tenha ocorrido algum desvio. Esse processo cíclico é executado constantemente e incrementa a qualidade da segurança e a gestão dos riscos.

O ciclo de segurança deve se iniciar com um planejamento, seguindo com o

desenvolvimento de protocolos, sistemas de detecção e resposta, treinamento e constante retroalimentação. É importante destacar que pelo fato de os eventos de segurança serem raros, deve haver treinamentos, simulados e testes para não se ter de lidar com surpresas.

Os controles de segurança da informação promoverão: defesa; intervenção; detecção e resposta; auditoria e auditoria forense; recuperação e intervenção preemptiva. Recordando as ideias de Gumpert et al. sobre mediação, novamente se fortalecer o paralelo entre a segurança e a mediação da informação, esclarecendo que a mediação é mais do que realizar o papel de canal na comunicação, ela envolve forças que influenciam o processamento humano da informação e molda interações sociais. Quando existir mediação com fim escuso deve haver uma contramedida, ação contra a mediação, de segurança da informação.

É por meio da exploração das vulnerabilidades que o malicioso se manifesta e se beneficia. O engenheiro social é aquele que consegue, por meio do abuso da confiança, obter proveito no âmbito da segurança da informação, comprometendo a autenticidade e a disponibilidade da informação, conseguindo acessá-la ou corrompendo-a. O engenheiro social faz a vítima do ataque pensar que ele é confiável e que as informações na posse da vítima não têm valor ou são inofensivas.[26]

Onde não há confiança surge a segurança. A segurança não é constituída puramente de tecnologia nem de mecanismos automatizados. Sua função é eliminar riscos para promover estabilidade e previsibilidade situacional. Mas nem sempre se pode prever, contar com a colaboração do outro e responder tempestivamente aos incidentes de segurança. Nesse momento, os métodos coercivos inibem transgressões, e a segurança será efetivamente proporcional ao método coercivo utilizado.

A segurança de pessoas resume-se basicamente ao desenvolvimento e à execução de protocolos. Se não há sujeitado a ser atacado não há problema de segurança. A eficiência do ataque está ligada ao ponto fraco do sistema. Por sua vez, a eficiência da segurança está relacionada a um encadeamento de contramedidas, mas não necessariamente ao seu número. As contramedidas devem ser independentes, pois na falha de uma outra deve atuar.

A compartimentação, ou seja, a segregação de funções, é uma forma eficiente de impedir que uma falha implique outra falha. É certo que as contramedidas testadas e validadas são muito mais eficazes que as novas e não testadas, especialmente com

[26] "*Always remember: amateurs hack systems, professionals hack people*." Bruce Schneier, CTO, Counterpane Internet Security, Inc. Dec 2000.

tecnologias complexas. A mente humana seria a melhor contramedida para manter a resiliência do sistema, mas, paradoxamente, em muitos casos ela constituir-se-ia no elo mais fraco da segurança e a causa de sua falha. Por conseguinte, a segurança será sempre um balanceamento entre os interesses dos envolvidos no contexto.

Por fim, um ataque bem-sucedido em segurança da informação combina técnicas e ferramentas em um contexto, conteúdo e usuários específicos. Se há interesse em elevar os níveis de segurança, deve-se primordialmente entender os interesses dos envolvidos e suas ideias sobre gestão de riscos.

Riscos e confiança são encontrados nas organizações e provavelmente com forte dimensão do CBT de Lewicki e Bucker nas comunicações formais de Baker. Por sua vez, KBT e IBT estão presentes nas comunicações informais de Baker. Portanto, o aprofundamento do conhecimento interpessoal por meio das comunicações leva ao aumento da confiança entre indivíduos, elevando os níveis de KBT e IBT.

Deduz-se que se confiança implica risco, risco de segurança da informação presume ameaça, ameaça se configura em possibilidade de ataque real, engenharia social é um tipo de ataque à segurança da informação, e quando não há sujeito a ser atacado – alvo – não há problema de segurança. A ARS possibilita a prospecção de possíveis alvos de ataques de engenharia social por analisar os riscos de segurança da informação. Deve-se mencionar que esses ataques se utilizam do abuso da confiança.

A confiança é um aspecto presente em uma terceira dimensão da segurança da informação e em todos os momentos no contexto organizacional. A segurança da informação está fundamentada na confidencialidade, na integridade e na disponibilidade. A confiança surge como um quarto elemento, influenciando todos esses outros elementos (**Figura *77***).

Acredita-se na teoria de Schneier: a segurança da informação é processo, e não produto. Ela não está ligada apenas à tecnologia, mas também a processos de trabalho e cuidados com as pessoas, ou seja, a segurança da informação está ligada ao comportamento seguro – a um comportamento obrigatório seguro. Por conseguinte, uma segurança efetiva é resultado do estabelecimento de modelos de comportamento obrigatório, por exemplo, políticas de segurança da informação.

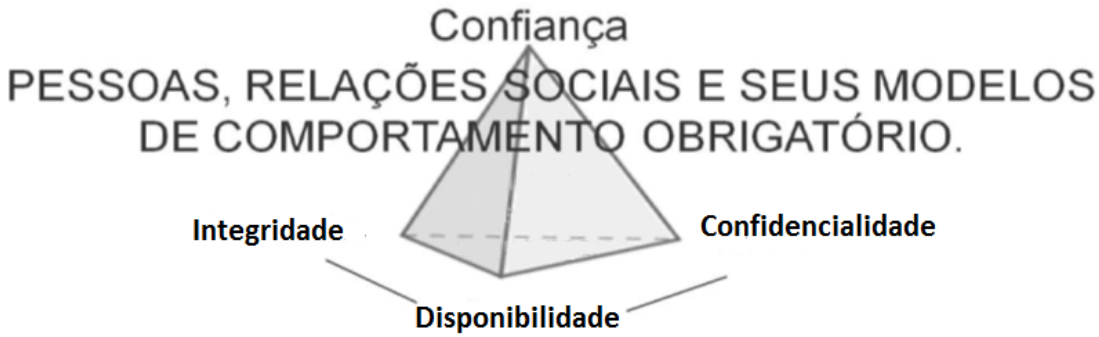


Figura 77. Relação entre a base da segurança da informação e a confiança

Como parte desta pesquisa foi feita uma coleta de dados no Portal da Transparência. Esses dados foram transformados em sociogramas para análise estrutural – que é a análise dos dados e dos sociogramas por meio da análise de redes sociais e relacionamentos – e cruzados com cenários de ataques de engenharia social. O método descrito neste trabalho possibilitou a identificação de potenciais alvos de forma mais objetiva e sistemática. Conseguiu-se demonstrar, de forma sucinta, que se pode ganhar escala e automatizar ataques dessa natureza.

É importante dizer que trabalhos dessa natureza dariam suporte à tomada de decisão em diversos aspectos da segurança da informação governamental. Por exemplo, daria melhor visibilidade ao impacto da publicação de informações no contexto das TIC em ambientes abertos, como o Portal da Transparência.

É claro que este método de identificação de alvos para engenharia social com ARS, apresentado neste trabalho, não esgota o assunto, mas apresenta uma linha de pensamento e abre possibilidades para novos estudos. Assim, a análise de redes sociais é uma boa ferramenta para explorar e analisar dados de segurança da informação.

Conforme foi visto, a análise de redes sociais não tem a capacidade de acabar com esse tipo de crime, mas é uma ferramenta que pode ser usada em conjunto com outras ferramentas nesse ofício e potencializar estratégias de combate. A ARS pode ajudar na tomada de decisão, mas não pode determiná-la. Como qualquer arma, pode ser usada para o bem ou para o mal.

Gráficos inteligíveis que representam fenômenos sociais relevantes a ataques de engenharia social, com base em métricas da análise de redes sociais, podem ser muito valiosos para a defesa. Fernandes defende a construção de um arsenal analítico para aprimorar a segurança da informação e das comunicações do Estado brasileiro.

Pelo exposto, infere-se que nesse cenário caótico e complexo podem ser

investigadas novas soluções para problemas cotidianos da segurança da informação, sem esquecer que as premissas do passado provavelmente podem ser usadas hoje. É importante o desenvolvimento de pesquisas para que se obtenha uma percepção da realidade de fato e a sociedade possa aprimorar, de forma evolutiva, sua segurança da informação.

Pode-se verificar que a análise de redes sociais no contexto dos estudos da confiança vem dividindo seus trabalhos no entendimento das redes de confiança, sua inferência a partir de dados coletados e a modelagem de sua propagação.

4.3 Limitações

Foram encontradas algumas limitações no desenvolvimento da pesquisa. O ideal seria realizar a pesquisa de opinião com instituições e servidores públicos cujos dados fossem coletados no Portal da Transparência, porém não houve oportunidade para tal.

O grau de confiança das relações não foi levantado por razões que serão explicitadas a seguir. Mas provavelmente seria possível medir o grau de confiança e apresentá-lo utilizando um modelo de confiança probabilístico, com pessoas e seus relacionamentos ou por meio de grafos sinalizados.

Apesar de a quantidade de dados e sua qualidade serem consideradas aceitáveis, é importante mencionar que não foi alvo da pesquisa construir um *software* ótimo, e que os eventuais erros do projeto talvez tenham influenciado a qualidade dos dados.

A coleta de dados foi prejudicada pela complexidade do *software*. Provavelmente por ter sido utilizada a rede *onion*, o tempo de resposta para as pesquisas no Portal da Transparência não foi tão rápido quanto se desejaria. O número de recursos computacionais não foi o ideal, uma vez que foi utilizado um computador do tipo *desktop* para hospedar máquinas virtuais, o que, de longe, não é um *hardware* desenvolvido para tal hospedagem de máquinas virtuais. O ideal seria conseguir servidores de virtualização e *storages* de dados.

Não foram realizados testes de intrusão nos órgãos, pois são prejudiciais e agressivos demais para o contexto de pesquisa acadêmica. Provavelmente teríamos resultados mais próximos da realidade se tivéssemos realizado testes diretos simulando ataques reais.

Everton (2013) declara que a análise de redes sociais não é a bala de prata contra as análises do crime, mas é uma ferramenta que pode ser usada em conjunto com outras ferramentas no ofício e potencializar estratégias de combate ao crime. A ARS pode ajudar na tomada de decisão, mas não pode determiná-la.

Portanto, esta pesquisa, a despeito de nossa opinião sobre sua qualidade, encontrou diversas limitações. Provavelmente com um patrocínio governamental poderíamos desenvolver conclusões mais assertivas e certezas mais concretas, comparadas aos resultados encontrados, os quais julgamos razoáveis, mas provenientes de recursos limitados.

4.4 Trabalhos futuros

Como apresentou Capurro, a semântica, o significado de um texto e documentos estão muito mais relacionados com teorias sobre língua e literatura, considerando que a informação está muito mais relacionada às teorias sobre computação e controle. Combinado com as ideias de Schneier sobre segurança por meio de uma intervenção preemptiva, pode-se perceber que é interessante pensar em um sistema que controle relações sociais inferindo e prevendo propagação de confiança e riscos associados utilizando a mediação da informação com *software* mais elaborados e estudados mais profundamente.

4.4.1 Aprimorar o web Scraping, Crawler e Parsing

4.4.1.1 Inferir confiança: cognição e mineração de dados

Mash (1994) apresenta uma tese para se inferir confiança utilizando Distributed Artificial Intelligence*.* Dastani et al. (2011) apresentam um estudo sobre a confiança como uma questão que emerge de muitas subáreas da inteligência artificial. Acredita-se que seria possível inferir confiança por meio das comunicações organizacionais.

4.4.1.2 Propagar confiança: previsão de bons e ruins estados de cooperação social

Jamali e Ester (2010) apresentam que os sistemas de recomendação e propagação da confiança são baseados nos efeitos seletivos e influência social condizentes com o fenômeno da homofilia, que é a tendência dos comuns agirem de forma similar e serem influenciados e influenciarem o grupo.

A análise da confiança em redes sociais envolve muitas variáveis. Como Huang et al. (2012) apresentaram, a confiança é um fenômeno complexo e um componente crítico das interações sociais humanas. Modelar confiança, sobretudo, é importante na análise de redes sociais, com aplicações no *marketing* viral, colaboração filtrada e segurança da informação.

4.4.1.3 Confiança e autorização

A segurança da informação, em geral, é entendida pela garantia de seus três aspectos fundamentais: a confidencialidade, que é a propriedade de a informação ser acessada por quem tenha autorização e não seja acessada por aqueles que não possuem autorização; a integridade, que é a propriedade de a informação não ter sido alterada por

qualquer agente desautorizado; a disponibilidade, que é o aspecto da segurança que garante que a informação estará disponível para todos os autorizados e que precisem dela sempre que necessário.

Se for possível se pensar em confiança como autorização, logo os três pilares da segurança da informação são “cravados” no terreno da confiança.

4.4.1.4 É possível generalizar um método de inferência e propagação dos riscos para o uso na segurança em geral

Imaginemos um sistema de informação que apresente possíveis relações de confiança sobre indivíduos e o conjunto destas relações sejam *Dark Networks*. Como um sistema dessa natureza a capacidade analítica e de tomada de decisão poderia ser útil para solução de investigações e prevenção de crimes.

Portanto, para evoluir os conhecimentos relacionados a este trabalho acreditamos que seria interessante aprimorar o *software* de extração, transformação, carga e análise dos dados para um *software* que contenha inteligência para inferir confiança nas comunicações e prever propagações dessa benesse na rede social. O Crawler, além de construir as redes sociais, poderia montar o *profile* dos atores da rede social, ou seja, identificação de alvo, seleção de *e-mail* preestabelecido para cada caso de exploração de vulnerabilidade e preenchimento de cada *e-mail* com os dados concretos coletados. A **Figura *78*** dá uma ideia melhor para essa abordagem.

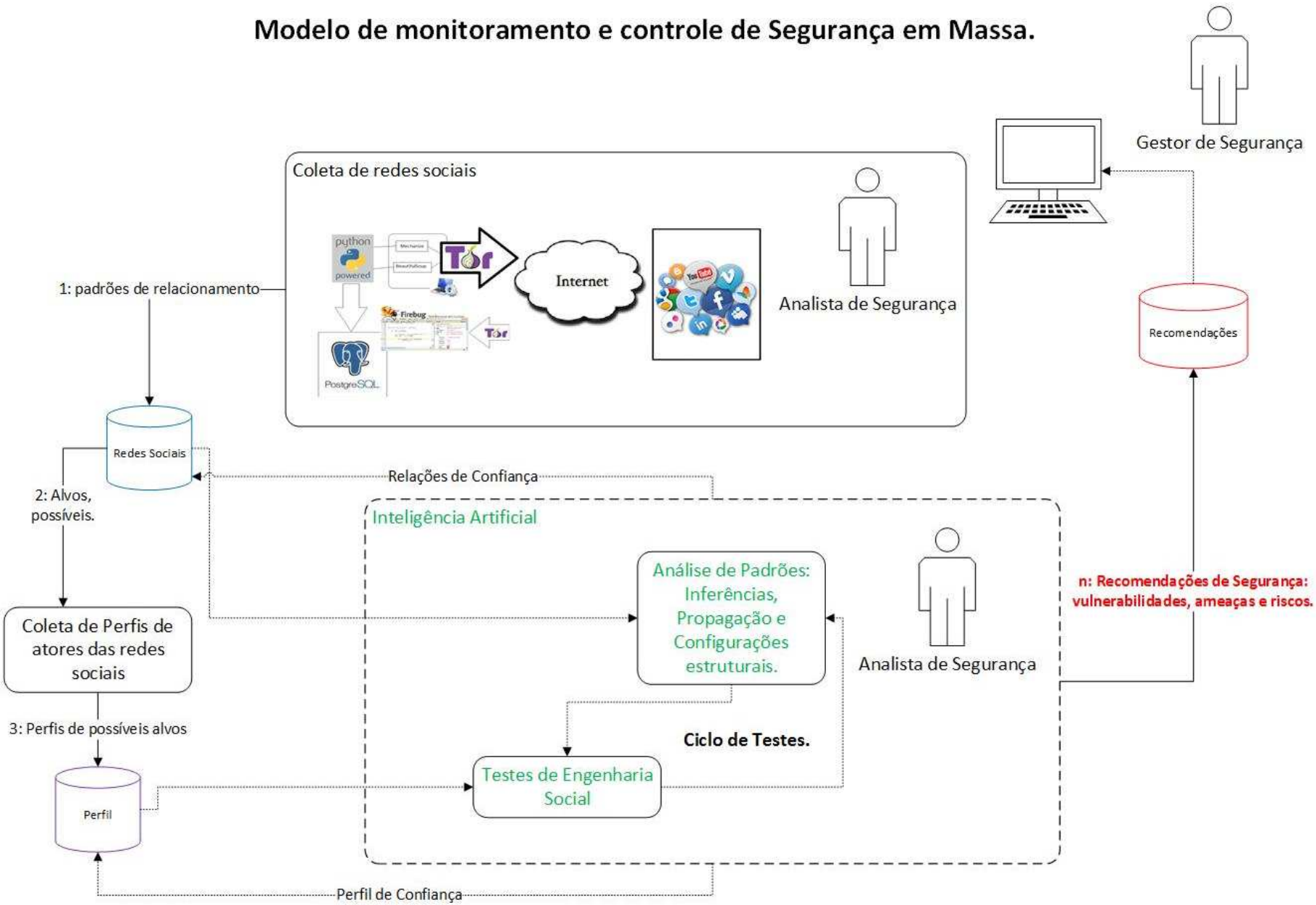


Figura 78. Modelo de uma possível implementação de sistema de controle para intervenção preemptiva, proativa.

Referências

ABDESSALEM, T.; CAUTIS, B.; SOUHLI, A. **Trust management in social network**. Paris: Télécom Paris Tech, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR/ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação**.Rio de Janeiro: ABNT, 2006.
———. **ABNT NBR ISO 31000**:. Gestão de riscos – Princípios e diretrizes. Rio de Janeiro: ABNT. 2009.

ALLEN, L. **Advanced penetration testing for highly-secured environments**: the ultimate secuty guide. Birmingham: Packt Publishing Ltd., 2012.

ALMEIDA, M. B.; CARNEIRO, L. E. S. Gestão da informação e do conhecimento no âmbito das práticas de segurança da informação: o fator humano nas organizações. **Revista Eletrônica de Biblioteconomia e Ciência da Informação**, Belo Horizonte, 2013.

AVIZIENIS, J.-C. et al. **Basic concepts and taxonomy of dependable and secure computing. Dependable and secure computing**, 2004.

AVIZIENIS, J.-C. LAPRIE. B. RANDELL, C. **Fundamental concepts of dependability**. [S.l.]:UCLA CSD Report, 2000.

BAKER, L. L. **Communication**. Boston: Pearson Education, 2002.

BATES, M. J. The invisible substrate of information science. **Journal of the American Society for Information Science**, v. 50, p. 1043-1050, 1999.
———. Information and knowledge: an evolutionary framework for information science. 239 f. **Information Research**, v. 10, 2005. Disponível em: <http://InformationR.net/ir/10-4/paper239.html>. Acesso em: 12 dez. 2014.

BERLO, D. **O processo de comunicação**: introdução à teoria e à prática. São Paulo: Martins Fontes, 2003.

BILL, J.; KLEIN, J. **Hacking work**: breaking stupid rules for smart results. Londres: Penguin Books, 2010.

BORDENAVE, J. D. **O que é comunicação**. São Paulo: Brasiliense, 1997.

BORKO, H. Information science: what is it? **American Documentation**, jan. 1968.

BROOKES, B. **The foundation of information science**. Part 1 – Philosophical aspects. J. Inf. Sc., p. 125-133, 1980.

CAPURRO, R. **What is information science for? A philosophical reflection**. Conceptions of library and information science. Historical, empirical and theoretical perspectives. Londres, p. 82-96, 1992. Disponível em: <http://www.capurro.de/tampere91.htm>.

CAPURRO, R.; HJØRLAND, B. The concept of information. **Annual Review of Information Science and Technology**, v. 37, p. 343-411, 2003. Disponível em: <http://www.capurro.de/infoconcept.html>.

CASTELFRANCHI, C.; FALCONE, R. **Social trust**: a cognitive approac. Unit of aI, cognitive modelling and interaction. Roma: National Research Council – Institute of Psycholog, 2001.

CHIAVENATO, I. **Introdução à teoria geral da administração**: uma visão abrangente da moderna administração das organizações. Rio de Janeiro: Elsevier, 2003.

CLAYBROOK, C. **Viewing organizational trust and internal auditing**. Dallas: The Institute of Internal Auditors (IIA), 2004.

COMMONS, C. **Obama issues executive order in support of open data**. Disponível em: <http://creativecommons.org/tag/open-data>. Acesso em: 16 ago. 2013.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de riscos corporativos**: estrutura integrada. Committee of Sponsoring Organizations. [S.l.]: The Committee of Sponsoring Organizations of the Treadway Commission, 2007.

COSTA, S. M. S.; LEITE, F. C. L. **Notas de aula da disciplina Fundamentos da Comunicação e Mediação da Informação**, 02/2013.

COSTA, S. M. S.; LEITE, F. C. L.; PIMENTA, S. G. **Notas de aula da disciplina Fundamentos da Ciência da Informação**, 01/2013.

CRESWELL, J. W. **Research design**: qualitative, quantitative, and mixed methods approaches. California: Sage Publications Inc., 2003.

DASTANI, M. et al. **Inferring trust**: the Netherlands and IRIT. Toulouse, 2011.

DAVALLON, J. **A mediação**: a comunicação em processo?, Vaucluse, 2003.

DE NOOY, W.; MRVAR, A.; BATAGELJ, V. **Exploratory social network analysis with Pajek**: structural analysis in the social sciences. 2. ed. New York: Cambridge Univerity Press, v. 1, 2011.

DOLAN, A. **Social engineering**. [S.l.]: Sans Institute. 2004.

DRETSKE, R. **Knowledge and the flow of information**. Cambridge, 1981.

EVERTON, S. F. **Disrupting dark networks (structural analysis in the social sciences)**. New York: Cambridge University Press, 2013.

FERNANDES, J. H. C. **Introdução à gestão de riscos de segurança da informação**: GSIC302 (notas de aula). 55 f. Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Brasília: Departamento de Ciências da Computação da Universidade de Brasília, 2010a.

———. **Sistemas, informação e comunicação**: GSIC050 (notas de aula). 51 f. Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Brasília: Departamento de Ciências da Computação da Universidade de Brasília, 2010b.
———. **Gestão da segurança da informação e comunicações**. 123 f. Brasília: Faculdade de Ciência da Informação, 2010c.
———. **Segurança da informação**: nova disciplina na Ciência da Informação? XI Encontro Nacional de Pesquisa em Ciência da Informação. Rio de Janeiro: [s.n.], 2010d.
———. **Segurança e defesa cibernética para reduzir vulnerabilidades nas infraestruturas críticas nacionais**. Brasília: Núcleo de Estudos Prospectivos da 7ª Subchefia do Estado-Maior do Exército Brasileiro, 2012.

FUKUYAMA, F. **Social capital and civil society**. IMF Working Paper. [S.l.]: International Monetary Fund. 2000.

GASQUE, K. C. G. D. **Letramento informacional**: pesquisa, reflexão e aprendizagem. Brasília: [s.n.], 2012.

GERCK, E. **Toward real-world models of trust**: reliance on received information, 1998. Disponível em: <http://mcwg.org/mcg-mirror/trustdef.htm>.

GERSTING, J. L. **Fundamentos matemáticos para a ciência da computação**. Rio de Janeiro: LTC – Livros Técnicos e Científicos Editora S.A., 1995.

GODINEZ, M. et al. **The art of enterprise information architecture**: A systems-based approach for unlocking business insight. Upper Saddle River: Pearson, 2010.

GRAGG, D. **A multi-level defense against social engineering**. [S.l.]: Sans Institute, 2002.

GUHA, R. et al. **Propagation of trust and distrust**. New York: IBM Almaden Research Center, 2004.

GULATI, R. **The threat of social engineering and your defense against it**. [S.l.]: Sans Institute, 2003.

GUMPERT, G. et al. **Mediation, information and communication**. London: Transaction Publishers, 1990. p. 21-36.

HADNAGY, C. **Social engineering**: the art of human hacking. Indianápolis: Willey Publishing Inc., 2011.

HILL, C. A.; O'HARA, E. A. **A cognitive theory of trust**. Twin Cities: University of Minnesota, 2005.

HUANG, B. et al. **Probabilistic soft logic for trust analysis in social network**. Maryland: University of Maryland, 2012.

KAUARK, F. D. S.; MANHÃES, F. C.; SOUZA, C. H. M. **Metodologia da pesquisa**: um guia prático. Itabuna: Via litterarum, 2010.

KOTHARI, C. R. **Research methodology, methods & techniques**. New Delhi: New Age International (P) Limited Publishers, 2004.

KROGERUS, M.; TSCHÄPPELER, R. **El libro de las decisiones, 50 modelos de éxito**: pequeño manual de deciosiones estratégicas. Buenos Aires: Pluma y Papel, 2011.

LA PORTA, R.; LOPEZ-DE-SILANES et al. Trust in large organizations. **The American Economic Association**, Cambridge, v. 87, p. 310-321, May 1997.

LASSWELL, H. D. The structure and function of communication in society. **The Communication of Ideas**. New York: Harper and Brothers, 1948.

LAZARTE, L. **A construção da sociedade da informação no Brasil**: avanços e entraves (1992-2002). Brasília: Universidade de Brasília (UnB), 2004.
———. **Ecologia cognitiva na sociedade da informação**. Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), 2000.

LOMBARDI, O. **What is information? Foundations of science**. Netherlands: Kluwer Academic Publishers, 2004. p. 1005-1034.

MACEDO, F. L. O. **Arquitetura da informação**: aspectos epistemológicos, científicos e práticos. 190 f. Dissertação (Mestrado em Ciência da Informação). Brasília: Universidade de Brasília (UnB), 2005.

MÄKINEN, H. **Risk, trust and security**. Knowledge of Society White Pape. Ann Arbor, 2005. Disponível em: <www.YhteiskunnanTieto.fi>.

MARAIS, J.; MOUTON, H. C. **Basic concepts**: in the methodology of the social sciences. 1. ed. Pretoria: HSRC Published, v. 1, 1996.

MARCIANO, J. L. P. **Segurança da informação**: uma abordagem social. 212 f. Tese. (Doutorado em Ciência da Informação). Brasília: CID/Face-UnB, 2006.

MARCIANO, J. L. P.; LIMA-MARQUES, M. O enfoque social da segurança da informação. **CI. Inf.**, Brasília, v. 35, p. 89-98, set./dez. 2006.

MARTELETO, R. M.; TOMAÉL, M. I. Redes sociais: posições dos atores no fluxo da informação. **Revista Eletrônica Biblioteconômica Ciência Informação**, Florianópolis, 1º sem. 2006.

MCALLISTER, D. J.; LEWICKI, R. J.; VEDI, S. C. **Trust in developing relationships**: from theory to measurement. Ohio: Ohio State University. 2006.

MCQUAIL, D; WINDAHL. S. **Communication models**. Singapura: Longman, 1993.

MIRANDA, A. **Ciência da Informação e a Teoria do Conhecimento Objetivo**: um relacionamento necessário. João Pessoa: Editora Universitária/UFPB, 2002. p. 9-24.
MITNICK, K.; SIMON, W. L. **The art of deception**: controlling the human element of security. 1. ed. Indianápolis: Wiley Publishing Inc., v. 1, 2002.

NASCIMENTO, M. S. O. D. **Proteção do conhecimento**: uma proposta de fundamentação teórica. Brasília: FCI/UnB, 2008.

OPEN DATA COMMONS. Making your data open: a guide open, 2013. Disponível em: <http://opendatacommons.org/guide/#sthash.K28tpib6.dpuf>. Acesso em: 16 ago. 2013.

PINHEIRO, L. V. R. Processo evolutivo e tendências contemporâneas da Ciência da Informação. **Informação & Sociedade**, João Pessoa, v. 15, n. 1, p. 13-48, jun. 2005.

RAUPP, F. M.; BEUREN, I. M. Metodologia de pesquisa aplicável às ciências sociais. In: BEUREN, I. M. **Como elaborar trabalhos monográficos em contabilidade**: teoria e prática. [S.l.]: Atlas, 2006. cap. 3, p. 76-97.

REALE, M. **Lições preliminares de direito**. 25. ed. São Paulo: Saraiva, v. 1, 2000.

RESSLER, S. Social network analysis as an approach to combat terrorism: past, present, and future research. **Homeland Security Affaris**, Sunderland, v. II, n. 2, jul. 2006. Disponível em: <www.hsaj.org>.

REZENDE, P. A. D. **Modelos de confiança para segurança em informática**. Brasília: Universidade de Brasília (UnB), 2011.

RIJSBERGEN, C. J. V. Information retrieval. **The Information Retrieval Group**. Glasgow: University of Glasgow, 1979.

ROSENFELD, L.; MORVILLE, P. **Information architecture for the world wide web**. 2. ed. [S.l.]: O'Reilly & Associates, v. 1, 2002.

RUBEN, D. B. **Between Commnunication & information, Information & Behavior**. London, Transaction Publichers, v. 4, p. 219-235, 1993.

RUSSELL, A. M. **Mining the social web**. 2. ed. USA: O'Reilly, 2013.

RYBCZYNSKI, W. **Information systems security user awareness**. Social Engineering and Malware. [S.l.]: Sans Institute, 18 November, 2000.

SACERDOTE, H. C. D. S.; FERNANDES, J. H. C. Investigando as interações em um ambiente virtual de aprendizagem por meio da análise de redes sociais. **Revista Ciência da Informação e Doc.**, Ribeirão Preto, v. 4, n. 1, p. 128-146, jan./jun. 2013.

SARACEVIC, T. Relevance: a review of and a framework for the thinking. **Journal of the American Society for Information Science**, v. 26, p. 321-343, Nov. Dec.1975.
———. Interdisciplinary nature of information science. **Ciência da Informação**, v. 24, n. 1, 1995.
———. Ciência da informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, p. 41-62, jan./jun. 1996.

SCHNEIER, B. **Secrets and lies**: the myth of security in the digital world. [S.l.]: John Wiley & Sons, 1998.

SCHNEIER, B. **Beyond fear**: thinking sensibly about security in an uncertain world. New York: Copernicus Books, 2003.
———. **Liars and outliers**: enabling the trust that society needs to thrive. Indianápolis: John Wiley & Sons, Inc., 2012.

SHANNON, C. A mathematical theory of communication. **Bell System Technical Journal**. [S.l.]: [s.n.], 1948.

SHOSTACK, A.; STEWART, A. **A nova escola da segurança da informação**. Rio de Janeiro: Alta Books, 2008.

SILVA, A. B. O.; FERREIRA, M. A. T. Gestão do conhecimento e capital social: as redes e sua importância para as empresas. **Informação & Informação**, Londrina, 2007.

SILVA, A. B. O. et al. **Análise de redes sociais como metodologia de apoio para a discussão da interdisciplinaridade na Ciência da Informação**. Belo Horizonte, 2005.

SILVA, D. P. E. **Vocabulário jurídico**. 26. ed. Rio de Janeiro: Forense, v. 1, 2006.

SILVA, P. A. L. **Análise de redes sociais aplicada à engenharia social**. Guaratinguetá: Faculdade de Tecnologia de Guaratinguetá, 2012.

SIQUEIRA, A. H. D. **Arquitetura da informação**: uma proposta para fundamentação e caracterização da disciplina científica. 402 f. Tese (Doutorado em Ciência da Informação). Brasília: Universidade de Brasília (UnB), 2012.

SLOMAN, A. **Information-processing systems in nature**, 2007. Disponível em: <http://www.cs.bham.ac.uk/research/projects/cogaff/sloman-information-nature.pdf>. Acesso em: 12 dez. 2014.

SOARES, R. H. S. **Métodos para análise da comunicação e mediação da informação em organizações públicas por meio de redes sociais mapeadas a partir de publicações oficiais**. Dissertação de Mestrado. Brasília: Universidade de Brasília (UnB), 2014.

SOUZA, R. C. D. **A auditoria de sistemas e segurança da informação em uma articulação normativa, ferramental e técnica**: estudo de caso em uma entidade da administração pública federal. 135 f. Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Brasília: Departamento de Ciências da Computação da Universidade de Brasília (CIC/UnB), 2011.

SWAN, W. et al. **A review of social network analysis for IMI trust in contruction project**. 17th Annual Arcom Conference. Salford: Association of Researchers in Construction Management, 2001. p. 59-67.

TUBBS, S. L. **Human Communication**: principles and contexts. 9. ed. New York: Mc Graw Hill, v. 1, 2003.

TURNER, J. H. **The structure of sociological theory**. 5. ed. Califórnia: University of California, v. 1, 1991.

TURNER, T. **Social engineering**: can organizations win the battle? Carolina: East Carolina University, 2005.

VALENTIM, M. L. P.; GELINSKI, J. V. V. Gestão do conhecimento como parte do processo de inteligência competitiva organizacional. **Informação & Sociedade**, João Pessoa, v. 15, n. 2, p. 1-12, jul./dez. 2005.

WASSERMANN, S.; FAUST, K. **Social network analysis**: methods and applications. 8. ed. New York: Cambridge University Press, v. 1, 1994.

WATSON, G.; MASON, A.; ACKROYD, R. **Social engineering penetration testing**: executing social engineering pen tests, assessment and defense. Oxford: Elsevier, 2014.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 4. ed. Porto Alegre: Bookman, 2010.

ZINS, C. Conceptions of information science. **Journal of the American Society for Information Science and Technology**, Jerusalém, v. 58, n. 3, p. 335-350, mar. 2007.
———. Knowledge map of information science. **Journal of the American Society for Information Science and Technology**, Jerusalém, v. 58, p. 526-535, jan. 2007b.

5 Glossário

Cibernética: é o estudo de fenômenos de controle, oscilação identificados a partir da análise do comportamento de sistemas mecânicos, sistema nervoso, fenômenos psíquicos, máquinas computacionais, sistemas autorreplicantes, sociedades humanas e animais.

Creative Commons: é uma organização não governamental sem fins lucrativos voltada a ampliar a quantidade de obras criativas disponíveis, por meio de suas licenças que autorizam a cópia e compartilhamento com menos restrições que o tradicional.

Objetividade: objetividade é a característica de um ente ser objetivo. Objetivo é proveniente do verbo latino *objecere* (pôr diante, apresentar). Objetivo quer dizer literalmente o vocábulo tudo o que é visível, concreto, real, positivo. Contrário à subjetividade, que se refere ao sujeito.

Organização: é o modo em que se organiza um sistema de administração e é desenvolvida por suas características de comando e controle. Facilitando, assim, o alcance de diversos objetivos, o alcance final de um objetivo que é o cerne da organização, sua missão. É uma forma de organização hierárquica com distribuição do trabalho por especialidades.

Outlier: é o valor em estatística aberrante ou valor atípico. É uma observação que apresenta um grande afastamento das demais da série. A existência de *Outliers* resulta, tipicamente, em prejuízos à interpretação dos resultados dos testes estatísticos aplicados as amostras. Na segurança da informação se trata do indivíduo que está fora da curva de comportamento, aquele que age puramente pensando em seus propósitos.

Persuasão: é uma estratégia de comunicação que consiste em utilizar recursos lógico-racionais ou simbólicos para induzir alguém a aceitar uma ideia, uma atitude, ou realizar uma ação. É o emprego de argumentos, legítimos ou não, com o propósito de conseguir que outro(s) indivíduo(s) adote(m) certa(s) linha(s) de conduta, teoria(s) ou crença(s). Segundo Aristóteles, a retórica é a arte de descobrir, em cada caso particular, os meios disponíveis de persuasão.

***Hacker*:** é um sujeito que se devota, com veemência rara, a desvendar e transformar os aspectos mais clínicos de dispositivos, sistemas e redes de computadores.

Apêndice A – Questionário da pesquisa de opinião

Pesquisa de opinião

Levantamento sobre confiança no ambiente de trabalho.

*Obrigatório

Parte superior do formulário

1. Qual seu nome completo?

Esta pergunta é opcional.

2. Qual seu local de trabalho?

Esta pergunta é opcional.

3. Como você considera sua prestatividade na sua unidade de trabalho? *

Por favor, utilize a escala de 0 a 5, sendo 0 nenhuma e 5 o máximo.

4. Quanto você considera a prestatividade algo importante para a eficiência das atividades laborais? *

Por favor, utilize a escala de 0 a 5, onde 0 é nenhuma e 5 é o máximo.

5. Quanto você considera sua prestatividade aos funcionários terceirizados na sua unidade de trabalho? *

Por favor, utilize a escala de 0 a 5, onde 0 é nenhuma e 5 é o máximo.

6. Seus superiores costumam delegar tarefas por telefone ou mensagem quando estão em compromissos fora de sua unidade de trabalho? *

- ○ Sim
- ○ Não

7. As empresas contratadas costumam receber informações para realizar suas tarefas fora de sua unidade de trabalho por telefone ou mensagem eletrônica? *

- ○ Sim

- [ ] Não

8. Já houve necessidade de acesso remoto aos equipamentos que você costuma trabalhar? *

- [ ] Sim
- [ ] Não

9. Todos os contratados que necessitam acessar os computadores que você trabalha são seus conhecidos? *

- [ ] Sim
- [ ] Não

10. Com que frequência você trabalha com contratados/terceirizados por telefone ou mensagem eletrônica? *

11. Quanto considera confiável seus contratados e/ou fornecedores? *

12. Você conhece algum caso de senhas serem enviadas por telefone ou mensagem eletrônica? *

- [ ] Sim
- [ ] Não

13. Você costuma receber listas de funcionários das contratadas periodicamente? *

- [ ] Sim
- [ ] Não

14. Há algum protocolo, onde teve a oportunidade de trabalhar, sobre procedimentos laborais com terceiros a sua unidade de trabalho? *

- [ ] Sim
- [ ] Não

15. Você sabe o que é classificação da informação? *

- [ ] Sim
- [ ] Não

16. Você já classificou alguma informação onde trabalhou? *

- [ ] Sim
- [ ] Não

17. Você sabe o que é engenharia social e já teve algum curso corporativo sobre o tema? *

- ○ Sim
- ○ Não

18. Você conhece alguém pessoalmente que já sofreu algum golpe, fraude ou crime via internet ou telefone, como ele relatou a experiência? *

19. Comentário. Escreva aqui sua experiência sobre classificação da informação, fraudes, golpes ou engenharia social na internet.
Campo não obrigatório.

Apêndice B – Trechos do código fonte da carga de dados

```
'''
Created on 16/06/2013

@author: raulc_000

CargaOrgaos.py

'''
import urllib ,urllib2
import time
import psycopg2
from BeautifulSoup import BeautifulSoup as bs_parse
from mechanize import Browser

BASE_URL = 'http://www.portaltransparencia.gov.br/despesasdiarias/resultado?consulta=avancada'
PERIODO_INICIO = '&periodoInicio='
PERIODO_INICIO_VALOR = '19%2F10%2F2010'
PERIODO_FIM = '&periodoFim='
PERIODO_FIM_VALOR = '18%2F11%2F2010'
FASE = '&fase='
FASE_VALOR = 'EMP'
CODIGO_OS = '&codigoOS='
CODIGO_OS_VALOR = '22000'
CODIGO_ORGAO = '&codigoOrgao='
CODIGO_UG = '&codigoUG='
CODIGO_UG_VALOR = 'TOD'
CODIGO_ED = '&codigoED='
CODIGO_ED_VALOR = 'TOD'
CODIGO_FAVORECIADO = '&codigoFavorecido='
SEARCH_URL = BASE_URL + PERIODO_INICIO + PERIODO_INICIO_VALOR + PERIODO_FIM + PERIODO_FIM_VALOR + FASE +
FASE_VALOR + CODIGO_OS + CODIGO_OS_VALOR
```

```
conn_string = "host='localhost' dbname='portaltransparencia' user='postgres' password='s4b3d0r14'"

br = Browser()

conn = psycopg2.connect(conn_string)

LRequest = urllib2.Request(SEARCH_URL," " )
LResponse = br.open(LRequest)
page = bs_parse(LResponse.read())
print SEARCH_URL
print page
#f.write(page)

br.close()

#cria array para orgaos superiores
print "################### Orgaos ###################"
a = []
b = []

cursor = conn.cursor()

cursor.execute("Select codigo from orgao_superior")

rows = cursor.fetchall()

for row in rows:
    a.append(row[0])

for cod in a:
    br = Browser()
    SEARCH_URL = BASE_URL + PERIODO_INICIO + PERIODO_INICIO_VALOR + PERIODO_FIM + PERIODO_FIM_VALOR + FASE
+ FASE_VALOR + CODIGO_OS + str(cod)
    LRequest = urllib2.Request(SEARCH_URL," " )
```

```
    LResponse = br.open(LRequest)
    page = bs_parse(LResponse.read())
    time.sleep(5)
    print SEARCH_URL
    for i in range(len(page('form'))):
        for j in range(len(page('form')[i]('select'))):
            if page('form')[i]('select')[j]['id'] == 'listaOrgaos':
                for k in range(len(page('form')[i]('select')[j]('option'))):
                    if page('form')[i]('select')[j]('option')[k]['value'] != 'TOD' and
page('form')[i]('select')[j]('option')[k].string != 'Todos' :
                        string = "INSERT INTO orgaos values(" + str(cod) + ',' +
page('form')[i]('select')[j]('option')[k]['value'] + ",'" +
page('form')[i]('select')[j]('option')[k].string + "');"
                        cursor.execute( string )
                        print string
    br.close()

#print b
conn.commit()
```

Apêndice C – Trechos do código fonte do coletor de dados

```
# -*- coding: utf-8 -*-
# ConsultasAvancadas.py

'''
Created on 24/01/2014

@author: raulc_000
'''

import urllib2
from BeautifulSoup import BeautifulSoup as bs_parse
from mechanize import Browser
import socks
import socket
from stem import Signal
from stem.control import Controller
import time
import random
import re
import sys
import logging, logging.handlers
from unicodedata import normalize
from idlelib.ReplaceDialog import replace

def remover_acentos(txt, codif='utf-8'):
    return normalize('NFKD', txt.decode(codif)).encode('ASCII','ignore')


def create_connection( address, timeout=None, source_address=None):
    sock = socks.socksocket()
    sock.connect(address)
```

```
    return sock

def gravalog(self, log):
    try :
        self.f.write(log + "\n")
        self.f.flush()
    except :
        print "Problemas ao gravar no arquivo"
        sys.exit()


def newID(self, controller):
    try :
        controller.signal(Signal.NEWNYM)
        aux = urllib2.urlopen("http://www.ifconfig.me/ip").read()
        print(aux)
        gravalog(self , aux + "\n")
        return aux
    except :
        time.sleep(random.choice(range(8,10)))
        controller.signal(Signal.NEWNYM)
        aux = urllib2.urlopen("http://www.ifconfig.me/ip").read()
        print(aux)
        gravalog(self , aux + "\n")
        return aux



class Consulta ():

    controller = None
    SEARCH_URL = None
    TOR_control_hostname = "127.0.0.1"
    TOR_control_port = "8118"
    TOR_control_password = "123456"
    contador = 0
    ID = ""
```

```
    ver = "4"
    arquivo = ''
    f = None


    def __init__(self, d_inic, m_inic, ano, search_url, controller, nao_cria):
        arquivo = '//home//raul//Documents//unb_python//data//data' + str(d_inic) + "-" + str(m_inic) + "-
" + str(ano) + '.txt'
        if nao_cria == 1:
            self.f = open(arquivo,'a')
        else :
            self.f = open(arquivo,'w')

        Consulta.controller = controller

        self.SEARCH_URL = search_url

        socks.setdefaultproxy(socks.PROXY_TYPE_SOCKS5, "127.0.0.1", 9050)

        # patch the PortalTransparecia module
        socket.socket = socks.socksocket
        socket.create_connection = create_connection

        br = Browser()

        #grava array com orgaos superiores
        print "################### Consulta Avancada Portal Transparencia ###################"
        gravalog(self,"\n\n\n################### Consulta Avancada Portal Transparencia ############\n\n")
        print "################### versao" + self.ver + " ###################"
        gravalog(self,"\n################### versao " + self.ver + " ###################\n\n")

        LRequest = urllib2.Request(self.SEARCH_URL," " )
        LResponse = br.open(LRequest)
        page = bs_parse(LResponse.read())
        print self.SEARCH_URL
        gravalog(self,self.SEARCH_URL + "\n")
        print page
```

```
        gravalog(self,(page.text).encode('ascii', 'ignore'))

        br.close()

#         Consulta.ID = newID(self, Consulta.controller)
        Consulta.ID = 000000000

        # Make a global logging object.
        x = logging.getLogger("logfun")
        x.setLevel(logging.DEBUG)

        # This handler writes everything to a file.
        h1 = logging.FileHandler("//home//raul//Documents//unb_python//data//log//erros" + str(d_inic) +
"-" + str(m_inic) + "-" + str(ano) + '.log')
        f = logging.Formatter("%(levelname)s %(asctime)s %(funcName)s %(lineno)d %(message)s")
        h1.setFormatter(f)
        h1.setLevel(logging.DEBUG)
        x.addHandler(h1)

    def _del_ (self):
        gravalog(self,"FIM!!!")
        self.f.close()



    def executa(self, search_url) :

        #try :
        self.SEARCH_URL = search_url

        list = [u'Favorecido:' , u'Valor:' , u'ObservaÃ§Ã£o do Documento:']

        socket.socket = socks.socksocket
        socket.create_connection = create_connection
        br = Browser()
        print search_url
```

```
    print "ID = " + str(Consulta.ID)
    gravalog(self,search_url + " cont = " + str(Consulta.ID) + "\n")
    LRequest = urllib2.Request(search_url," " )
    LResponse = br.open(LRequest)
    page = bs_parse(LResponse.read())

    # pode ir para fora!!!!

    soup = bs_parse(LResponse.get_data())
    img_captcha = soup.find('img', alt='captcha')
    if img_captcha != None :
        try:
            print "CAPTCHA!!!"
            gravalog(self,"CAPTCHA\n")
        finally:
            Consulta.ID = newID(self, Consulta.controller)
            br.close()
            socket.socket = socks.socksocket
            socket.create_connection = self.create_connection
            br = Browser()
            print search_url + " cont = " + str(Consulta.ID)
            gravalog(self,search_url + " cont = " + str(Consulta.ID) + "\n")
            LRequest = urllib2.Request(search_url," " )
            LResponse = br.open(LRequest)
            page = bs_parse(LResponse.read())
    entra = 0
    for table in page.findAll("table"):
        for row2 in table.findAll('tr'):
#             print row2
            for col in row2.findAll('td'):
                for href in col.findAll('a'):
                        print href
                        gravalog(self,str(href).encode('ascii', 'ignore') + '\n')
                        #resp = br.follow_link(text_regex=href.string)
                        #html = resp.read()
                        #print html
                if col.string != None :
```

```
m = re.search('a href', col.string)
if m != None :
    print 'Link!!!'
    gravalog(self,'Link!!!\n')
    print col.string
    gravalog(self,str(col.string).encode('ascii', 'ignore') + '\n')
m = re.search('INFORMATICA', col.string)
if m != None :
    entra = 1
m = re.search('TELECOMUNICACOES', col.string)
if m != None :
    entra = 1
m = re.search('TELECOMUNICACAO', col.string)
if m != None :
    entra = 1
m = re.search('NETWORKS', col.string)
if m != None :
    entra = 1
m = re.search('NETWORK', col.string)
if m != None :
    entra = 1
m = re.search('REDE', col.string)
if m != None :
    entra = 1
m = re.search('REDES', col.string)
if m != None :
    entra = 1
if entra == 1 :
    logfun = logging.getLogger("logfun")
    logfun.debug("Inside f!")
    try :
        print 'BINGO!'
        gravalog(self,'BINGO!\n')
        print href.string
        gravalog(self,str(href.string).encode('ascii', 'ignore') + '\n')
        LResponse = br.follow_link(text_regex= href.string)
        html = LResponse.read()
```

```
                                print html
                                gravalog(self,html + '\n')
                                page = bs_parse(html)
                                cont = 3
                                for table in page.findAll("table"):
                                    for row2 in table.findAll('tr'):
                                        #            print row2
                                        favorecido = 0
                                        valor = 0
                                        observacao = 0
                                        for col in row2.findAll('td'):
                                            if favorecido == 1 :
                                                texto = str(col.string).encode('ascii',
'ignore').replace("'", "").replace(";", "").replace("--", "")
                                                print texto
                                                gravalog(self,texto + '\n')
                                                list.append(texto)
                                            if valor == 1 :
                                                texto = str(col.string).encode('ascii',
'ignore').replace("'", "").replace(";", "").replace("--", "")
                                                print texto
                                                gravalog(self,texto + '\n')
                                                list.append(texto)
                                            if observacao == 1 :
                                                texto = str(col.string).encode('ascii',
'ignore').replace("'", "").replace(";", "").replace("--", "")
                                                print texto
                                                gravalog(self,texto + '\n')
                                                list.append(texto)
                                                print list
                                            if col.string != None :
                                                m = re.search(u'Favorecido:' , col.string)
                                                if m != None :
                                                    print u'Favorecido:'
                                                    gravalog(self, u'Favorecido:' )
                                                    favorecido = 1
                                                m = re.search(u'Valor:' , col.string)
```

```
                                        if m != None :
                                            print u'Valor:'
                                            gravalog(self, u'Valor:' )
                                            valor = 1
                                        m = re.search(u'ObservaÃ§Ã£o do Documento:' , col.string)
                                        if m != None :
                                            print u'ObservaÃ§Ã£o do Documento:'
                                            gravalog(self, u'ObservaÃ§Ã£o do Documento:' )
                                            observacao = 1

                                    entra = 0
                                    br.back()
                                except Exception, ex:

                                    logfun.exception("\nSomething awful happened! \n" + search_url)

                                logfun.debug("Finishing f!")
                                    #sys.exitPortalTranspareciaef)
                                    #print col.string
                                    #print col
                                    #print row2

        br.close()
        return list
#         except :
#             print Exception
#             print 'problema com : ' + search_url
#             sys.exitPortalTransparecia
```

Apêndice D – Trechos do código fonte criador de rede para o Pajek

```
# -*- coding: utf-8 -*-
# Cria_net_pajek.py

'''
Created on 05/03/2014

@author: raulc_000
'''
import psycopg2
import sys
from ConsultasAvancadas import gravalog

f = None

def gravaArquivo(f, texto):
    try :
        f.write(texto + "\n")
        f.flush()
    except :
        print "Problemas ao gravar no arquivo"
        sys.exit()

arquivo = 'C:\\Users\\raulc_000\\Documents\\data\\rede_pajek.net'
f = open(arquivo,'w')

conn_string = "host='localhost' dbname='portaltransparencia' user='postgres' password='s4b3d0r14'"

conn = psycopg2.connect(conn_string)

cursor = conn.cursor()
```

```
stringSQL = "select DISTINCT(ug.codigo), ug.descricao    from unidade_gestora as ug, consulta as con"
stringSQL =  stringSQL +  " where ug.codigo = con.unidade_gestora order by ug.codigo;"

cursor.execute(stringSQL)

rows = cursor.fetchall()

dict = {}

count = 1
for row in rows:
    aux = row[1]
    dict[aux] = count
    count = count + 1

aux2 = len(dict)

stringSQL = "select DISTINCT(favorecido) from consulta;"

cursor.execute(stringSQL)

rows = cursor.fetchall()

for row in rows:
    aux =  row[0]
    dict[aux] = count
    count = count + 1


d = sorted(dict, key=lambda x : dict[x])

print "*Vertices " + str(len(d)) + " "  + str(aux2)
gravaArquivo(f,"*Vertices " + str(len(d)) + " "  + str(aux2))

for x in d:
    print "%s \"%s\"" % (dict[x], x)
    gravaArquivo(f,"%s \"%s\"" % (dict[x], x))
```

```
print "*Edges"
gravaArquivo(f,"*Edges")

stringSQL = "select ug.descricao, con.favorecido from unidade_gestora as ug, consulta as con "
stringSQL =  stringSQL + "where ug.codigo = con.unidade_gestora order by ug.codigo;"

cursor.execute(stringSQL)

rows = cursor.fetchall()

for row in rows:
    print str(dict[row[0]]) + " " + str(dict[row[1]])
    gravaArquivo(f,str(dict[row[0]]) + " " + str(dict[row[1]]))

arquivo2 = 'C:\\Users\\raulc_000\\Documents\\data\\rede_pajek_partition.clu'
f2 = open(arquivo2,'w')

print "*Vertices " + str(len(d))
gravaArquivo(f2,"*Vertices " + str(len(d)))

for x in d:
    if int(dict[x]) <= int(aux2):
        print "1"
        gravaArquivo(f2, "1")
    else :
        print "2"
        gravaArquivo(f2, "2")
```