UM ESTUDO SOBRE A CONFIANÇA EM SEGURANÇA DA INFORMAÇÃO FOCADO NA PREVENÇÃO A ATAQUES DE ENGENHARIA SOCIAL NAS COMUNICAÇÕES DIGITAIS

The study's role of trust on information security with an interdisciplinary approach on social engineering prevention

Jorge Henrique Cabral Fernandes (1), Raul Carvalho de Souza (2)

(1) Universidade de Brasília, jhcf@unb.br. (2) Procuradoria Geral do Distrito Federal, raul.carvalhodesouza@gmail.com

Resumo

O estudo investiga definições práticas a respeito da confiança e seus riscos. Empregando a análise de redes sociais (ARS) com base em dados publicados em portais de transparência identifica vulnerabilidades a ataques de engenharia social. O artigo insere-se no debate sobre estudos dos aspectos objetivos e subjetivos para o estabelecimento da confiança interpessoal organizacional. A confiança implica riscos na segurança da informação (SI) e na segurança cibernética. A violação das propriedades básicas de segurança da informação proveniente do abuso da confiança causa um prejuízo organizacional, e isso implica em necessidade de aumento da consciência situacional pelas entidades cujos dados se encontram em portais de transparência. Foram identificadas e analisadas comunicações registradas em bancos de dados abertos sobre aquisições de produtos e serviços de informática, disponíveis no Portal da Transparência do Governo Federal. Foram identificados potenciais alvos para a realização de ataques de engenharia social. As possibilidades de ataques de engenharia social foram comprovadas por levantamento baseado em questionários com foco nas comunicações digitais de voz e dados, seja por mensagens eletrônicas (e-mails) ou por meio de mensagens curtas – SMS, WhatsApp –, telefonia, entre outros.

Palavras-chave: Confiança, Risco. Segurança, Informação, Consciência Situacional.

Abstract

The study investigates practical definitions regarding the trust and its risks. Uses social network analysis (SNA) for vulnerability analysis in social engineering. The article is part of the debate on studies of objective and subjective aspects for the establishment of organizational interpersonal trust. Trust implies risks in information security (IS) and cyber security. Violation of basic properties of information security from the trust abuse causes organizational loss. They were identified and analyzed the information and communications flows using ARS as a tool applied on open data from the Portal da Transparência do Governo Federal. Was identified potential targets for performing social engineering attacks. The possibilities of social engineering attacks have been proven by research based on questionnaires focusing on digital voice and data communications, whether by electronic mail (e-mail) or through short messages - SMS, WhatsApp – telephony and others.

Keywords: Trust, Risk, Security, Information. Situational Awareness.

1. Introdução

O artigo procura responder à questão de como podem ser identificados alvos para ataques de engenharia social (ES), no que se refere ao abuso de confiança no uso de comunicações digitais. Utiliza como ferramenta a análise de redes sociais (ARS) aplicada em dados abertos obtidos junto a sítios na web, mais especificamente no Portal da Transparência do Governo Federal. O artigo analisa as redes sociais modeladas sobre casos concretos de aquisições públicas, para encontrar possíveis alvos de ataques de engenharia social. A possibilidade de mediação feita por sistema de comunicação da informação– intermediação – permite obter insights sobre riscos de ataque e possivelmente aplicar recomendações normativas em prevenção para a segurança da informação (SI). Esses insights permitem aumento da consciência situacional (Endsley, 1995) pelas entidades cujos dados abertos se encontram publicados. Não é abordado o problema específico do sigilo da comunicação de dados na Internet, mas sim os riscos

relativos a ataques de engenharia social decorrentes da exploração de dados de redes sociais humanas cujos relacionamentos se encontram registrados em bancos de dados públicos acessíveis por sítios web. Segundo Endsley a Consciência situacional é "a base primária para a tomada de decisão e desempenho na operação subsequente de sistemas complexos". Nesse caso, a tomada de decisão é a adoção de controles para fortalecimento da autenticidade em comunicações digitais, diante da complexidade dos sistemas de dados abertos do Estado.

O trabalho surgiu de uma pesquisa de mestrado de aluno do Programa de Pós-Graduação em Ciência da Informação (PPGCINF) da Universidade de Brasília (UnB), um dos autores desse artigo. A pesquisa foi feita com a finalidade de encontrar objetividade (1) sobre a confiança e o risco, no tema segurança da informação e segurança cibernética (2), sem desprivilegiar os aspectos subjetivos correlatos ao tema. Nela, se defende que é um desafio complexo e contemporâneo determinar aspectos objetivos sobre confiança e risco em Segurança da Informação.

Entende-se ser necessário utilizar conhecimentos de várias disciplinas para estudar o fenômeno. Há demanda para se compreender claramente o que são a informação, a segurança, os aspectos objetivos e comportamentais nas relações interpessoais, entre outros conceitos, em um mesmo contexto. Isso permite encontrar respostas aos desafios do dia a dia da SI (Fernandes, 2010; Schneier, 2012; Command Five Pty Ltd, 2011).

A saída para investigar problemas conexos ao comportamento de atores no espaço cibernético demanda que se pesquisem em múltiplos autores de ciências distintas, conceitos para permitir apreender e almejar uma concordância científica (Fernandes, 2010; Saracevic, 1995; Silva et al., 2005). Nesses diferenciados nichos científicos novas óticas sobre as organizações sociais precisam ser destacadas para auxiliar a SI. Esse trabalho defende uma visão estrutural e comportamental dos indivíduos dessas organizações sociais.

Lazarte (2000) chancela a existência de novos desafios nesse mundo novo: "Além da dimensão econômica e suas implicações, a Sociedade da Informação traz mudanças na forma em que interpretamos o mundo, impacta nosso ambiente interior e põe novos desafios a nossas relações sociais". Para Schneier (2012), a tecnologia mudou a forma com que nossas interações sociais ocorrem, mas, segundo ele, é muito fácil esquecer isso. É importante mencionar que Fernandes (2012) defende a construção de um arsenal analítico para aprimorar a segurança do Estado.

2. Metodologia

A pesquisa em tela é aplicada, qualitativa, diacrônica e descritiva. Suas técnicas de coleta e análise de dados são o estudo de caso e a análise de redes sociais (ARS). Trata-se de uma pesquisa quase experimental, pois, apesar de desenvolver testes e experimentos, o pesquisador não tem controle total sobre o ambiente.

A ARS foi a metodologia de análise dos dados preferencialmente empregada na pesquisa. Além de verificar estruturalmente a manifestação das relações sociais, ela permite extrair conclusões sobre o comportamento de grupos de pessoas que compõem uma rede social. Com a ARS é possível ponderar sobre o fluxo das informações que circulam na rede social em análise. O estudo de caso foi utilizado para exibir os riscos de ataque. Esses riscos foram corroborados por entrevistas com servidores e empregados de organizações públicas, a fim de enquadrar os casos concretos aos cenários estudados nas bibliografias.

Diversas coletas automatizadas no Portal da Transparência foram feitas com o uso de um software construído para esse fim. Os dados sobre aquisições de bens e serviços de informática foram armazenados em uma base de dados relacional. Os dados coletados foram transformados em modelos de redes sociais para que pudesse ser feita a análise de redes sociais apoiada pelo software Pajek (3).

Em outra fase metodológica foi feito um levantamento de percepções, no qual servidores públicos foram consultados sobre possíveis vulnerabilidades no que diz respeito à autenticação da informação digitalmente comunicada. O propósito foi efetuar um cruzamento das percepções dos servidores sobre o tema, conhecer suas experiências com fraudes e verificar possíveis brechas no contexto social, para a ocorrência de ataques em engenharia social. A evidenciação dessas brechas permite melhor desenvolvimento da consciência situacional dos que habitam o espaço cibernético.

A validade do construto dá legitimidade qualitativa à pesquisa. Uma propriedade fundamental dos testes na validade de um construto é a convergência, ou seja, os resultados dos diferentes testes devem convergir. Diferentes testes podem denotar diferentes fontes de informação. Portanto, para criar maior convergência entre as afirmações apresentadas diante da questão de pesquisa (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?), foram consultados 45 agentes públicos lotados nas 14 organizações listadas a seguir: Bacen – Banco Central do Brasil; CD – Câmara dos Deputados; CEF – Caixa Econômica Federal; CN – Congresso Nacional; Dataprev – Empresa de Tecnologia e Informações da Previdência Social;

Dftrans – Secretaria de Transporte do Distrito Federal; GSIPR – Gabinete de Segurança Institucional da Presidência da República; Infraero – Empresa Brasileira de Infraestrutura Aeroportuária; PGR – Procuradoria-Geral da República; PMDF – Polícia Militar do Distrito Federal; PGDF – Procuradoria-Geral do Distrito Federal; Serpro – Serviço Federal de Processamento de Dados; SEDF – Secretaria de Educação do Distrito Federal, além de uma que não quis ser identificada.

A Figura 1 sumariza o processo metodológico da pesquisa. Os pressupostos em ciência da informação, da segurança da informação, da engenharia social, da confiança e da análise de redes sociais dão base para a aplicação do método de coleta e análise, gerando dados para uma possível apresentação de alvos de ataques de engenharia social e, por conseguinte, promover prevenção de ataques a esses alvos, com aprimoramento da consciência situacional.

A base conceitual possibilita 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 normas e nas bibliografias, apresentam-se caminhos para a prevenção de ataques de engenharia social, por meio de desenvolvimento de consciência situacional.

3. Fundamentação

3.1 Ataques de engenharia social

Os ataques à segurança da informação (SI) por meio de dados obtidos na Internet estão ficando cada vez mais avançados e complexos (Command Five Pty Ltd, 2011), sendo a engenharia social (ES) uma preocupação cada dia mais forte. Atualmente, os ataques persistentes avançados (APA) estão combinando diversos vetores de ataque para chegar aos seus objetivos.

O termo APA é usado no contexto de cyber ameaças (ou cyber ataques). O hacker (4) no APA possui habilidades suficientes para um ataque bem-sucedido, e não apenas a intenção. Essas habilidades devem ser avançadas para o contexto informacional do ataque. O APA é persistente porque não há precipitação no ataque, havendo, sim, bastante cautela e cálculo (Command Five Pty Ltd, 2011). Diversos APAs utilizam como primeira milha de ataques a engenharia social; o Tabela I apresenta uma lista alvos de APA em 9 organizações, ocorridos nos intervalos de 1998 a 2011.

Nota-se, portanto, que engenharia social é um dos vetores mais utilizados em Ataques Persistentes Avançados. O que se quer evidenciar é que se a engenharia social presume confiança, e confiança pode ser observada por meio das comunicações, provavelmente mecanismos para evitar ataques de engenharia social podem ser criados com estudos interdisciplinares, auxiliados pela ARS e pelo estudo de casos.

Organizações alvos de ataques	*Método*
OAK Ridge National Laboratory; Los Alamos National Laboratories; GhostNet; Night Dragon; Operation Aurora; The French Finance Ministery; Canadian Government e RSA	E-mails de engenharia social

Tabela I. *Alguns ataques persistentes avançados (APA) com engenharia social e perda de dados Fonte: Command Five Pty Ltd. (2011)*

Para Mitnick e Simon (2002) um ataque de engenharia social é uma ação elaborada que explora o altruísmo e a boa vontade das pessoas. Esses autores acreditam que a engenharia social coloca o atacante em uma posição privilegiada no fluxo da informação, de forma que o trapaceiro alcance seus objetivos. Os autores afirmam ainda que a ES se aproveita do abuso da confiança para conseguir seus fins. A consciência situacional sobre esses fluxos privilegiados de informação permite redução dos riscos de abuso da confiança.

3.2 Fluxos de informação e papéis sociais

O fenômeno da confiança interpessoal nas organizações é uma incógnita para a ciência. Não se identifica uma forma precisa de observar esse fenômeno, pois nele se cruzam aspectos objetivos e subjetivos, o que requer observação tanto de aspectos exógenos, quanto endógenos dos indivíduos para seu entendimento (Rezende, 2011; Hill e O'Hara, 2005). A intensificação do uso de sistemas de comunicação digital tem tornado o cenário da confiança interpessoal bastante mutante e complexo.

Para se identificar e analisar em uma organização (5) os fluxos de informações, Silva et al. (2005) sugerem o uso da análise de redes sociais (ARS). A verificação computacional do comportamento das relações sociais de indivíduos ou de um grupo organizacional é possível com a ARS. As redes sociais geralmente podem ser modeladas matematicamente. Sociogramas (grafos, no sentido matemático) podem ser estudados por meio de termos e conceitos ou processos relacionais (De Nooy et al., 2011; Wassermann and Faust, 1994).

A condução e a difusão de vários tipos de benesses materiais e não materiais numa rede social, para Everton (2013), podem ser estudadas com ARS. Dentre essas benesses estão **informações** e **confiança**. Ressler (2006) defende que a prática da ARS é a base de uma nova inteligência necessária para os assuntos de segurança. Com a ARS podem ser avaliados relacionamentos sociais entre indivíduos, de forma que se identifiquem papéis e comportamentos ao longo do tempo.

O sociólogo Simmel utiliza a análise de tríades como base para a análise de troca de valor em redes sociais. As tríades incompletas (onde falta o relacionamento entre dois atores) de relacionamento possibilitam a um dos atores sobre os demais da relação o controle e exploração de sua posição na rede, por meio da condição favorável na relação com assimetria estrutural (De Nooy et al., 2011; Wolff, 1950).

Essa exploração da assimetria estrutural possibilita o desempenho de papéis de corretagem (brokerage roles). Existem diversos papéis de corretagem em tríades incompletas. Observando-se as cinco tríades na Figura 2, cada vértice (v, u, w) representa um ator e as setas indicam o fluxo da informação. As linhas circulares delimitam atores que pertencem a um mesmo grupo. O ator que encontra-se na parte superior das tríades pode controlar a comunicação. Pode-se verificar o papel do coordenador na tríade mais à direita, que é um mediador integrante de um mesmo grupo. No segundo papel, o corretor itinerante é intermediário de dois membros de um mesmo grupo, vértices "u" e "w", mesmo estando ele fora do grupo. Na terceira tríade, o mediador atua como um representante, podendo regular o fluxo de informações ou recursos que saem de um lado a outro. Na quarta tríade, o porteiro (gatekeeper) pode apenas regular o fluxo de informações ou benesses entrantes em um grupo do qual ele não participa. Por fim, o ligador ou conector é quem media o fluxo de benesses entre dois grupos (De Nooy et al., 2011).

3.3 Modelos de comportamento obrigatório e o hacker

Em outra linha de pensamento, o formalismo, a matemática e os grafos não são a panaceia. Lá não residem as respostas para todos os problemas de SI.

> 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 (Shostack and Stewart, 2008, p. 49).

Diversos problemas em segurança da informação são proveitosamente iluminados pela matemática e pela lógica. Porém, uma vez resolvidos, surgem questões onde computadores, normas sociais e o comportamento das pessoas se cruzam (Shostack and Stewart, 2008). Segundo Saracevic (1995), a Ciência da Informação tem um forte viés social e humano, mas não rompe relações com as ciências hard. O jurista Reale apresenta os modelos de comportamento social obrigatório:

> 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 obrigatórios** (Reale, 2000, p. 186, grifo nosso).

No contexto da segurança da informação, modelos (6) de comportamento obrigatório, assim como define Reale, são dignos de estudo e análise. Sua materialização está nas normas internacionais, nas leis, nas políticas, nas instruções normativas, nas normas complementares, nos manuais de boas práticas, nos processos organizacionais, nos protocolos de segurança, nos fluxos de trabalhos etc. Quando esses são criados, conjecturam relações sociais salutares, vislumbram uma sociedade justa ou uma organização saudável.

Os modelos de comportamento obrigatório constituem barreiras para o hacker e seus alvos. De acordo com Mäkinem (2005), a segurança, sobretudo, cria condições para a existência de atividades sociais de grande escala no tempo e no espaço. O hacker, por exemplo, não quer seguir a política de segurança da informação de uma organização quando ela impede seu objetivo ou interesse. Uma sociedade em constante evolução sempre deve acompanhar os resultados de seus enquadramentos comportamentais, consultando as pessoas e aprimorando seus modelos de comportamento obrigatório. Para isso é preciso controle e inteligência.

3.4 Monitoramento e controle social

O controle e o monitoramento são parte integrante da segurança, parte do sistema administrativo social e são baseados no armazenamento de informações da conduta das pessoas (Mäkinem, 2005). Para se garantir o estado das coisas, são necessários o controle e o monitoramento. A supervisão direta da conduta das pessoas é item do controle. A supervisão da conduta em uma organização é essencial, pois sem ela não há qualidade nos processos. Mas é perigoso permitir a qualquer um ter o controle das informações sobre as relações sociais.

Nessa linha, a Internet é um ambiente aberto e de controle complicado. Mäkinen (2005) afirma que a Internet, a rede mundial de computadores, é uma rede caótica. Nas redes caóticas as pessoas participam de suas atividades e não têm ideia do tipo de controle que

essas informações recebem. Essas informações podem ser usadas para interesses comerciais, controle de opinião, entre outras finalidades. Castelfranchi e Falcone (2001) ratificam o surgimento de técnicas de detecção e prevenção de fraudes e tendem a considerar a confiança estabelecida nos ambientes com redes eletrônicas. Os autores afirmam que confiar é arriscar-se, portanto confiar implica risco. Swan et al. (2001) afirmam que a confiança é desenvolvida com base na comunicação e nas ações.

Portanto, dos fundamentos conceituais até aqui apresentados, pode-se concluir que com a ARS é feita uma análise eficiente sobre uma grande quantidade de dados abertos e provavelmente podem ser verificadas as relações de confiança, posto que essas relações de confiança são formadas por meio das comunicações. Com as relações de confiança expostas, talvez pudessem ser apontadas vulnerabilidades e possíveis alvos da engenharia social. A seguir são verificados os resultados e a análise dos dados coletados na pesquisa.

4. A publicação das informações na Internet e a exploração da confiança em meio digital

O contexto atual da segurança da informação nas organizações com informações na Internet pode ser considerado crítico, pois as possibilidades de engenharia social são aparentes. Talvez a situação seja agravada devido ao princípio governamental da publicidade, que muitas vezes se choca com as políticas de segurança da informação. O pressuposto da pesquisa foi que devido à grande exposição de informações públicas sobre organizações na Internet, seriam possíveis ações remotas de coleta de dados abertos, para facilitar seleção de alvos para ataques em engenharia social. O modelo das tríades encontradas nas redes pesquisadas poderia ser explorado com o abuso da confiança e o uso dos papéis de corretagem da ARS.

O uso de consultas aos entes inseridos no contexto informacional é um estudo do ponto de vista do usuário e promove uma visão subjetiva da situação, proporcionando outro viés de verificação e da validade das informações coletadas automaticamente e analisadas objetivamente. A visão dos usuários da informação, do ponto de vista de suas necessidades de segurança da informação promove uma melhor contextualização da informação.

4.1 Levantamento sobre o cuidado com a autenticidade

O levantamento realizado com 45 servidores públicos mostra despreocupação com a autenticidade da comunicação digital. Como pode ser observado na Figura 3, 82% dos consultados na pesquisa recebem ou enviam tarefas por e-mail, possibilitando o uso desse canal para ataques de engenharia social, por exemplo, com a personificação (7). Na Figura 4 constata-se que 60% dos consultados precisaram enviar informações restritas por e-mail, por exemplo, senhas para executar suas tarefas durante suas atividades de trabalho.

Além disso, 69% dos consultados já tiveram seu computador acessado remotamente, e mais da metade não conhecia quem fez esse acesso. Na Figura 5 nota-se o grau de confiança depositado pelos respondentes nos fornecedores e nos terceirizados. A pesquisa considerou uma escala de 0 a 5, onde 0 é não confiar e 5 é confiança total. Provavelmente, em uma situação dessas, a regra de "necessidade de saber" (8) não é seguida, porque 47% confia muito ou totalmente em terceiros. É importante dizer que a solução não é desconfiar de terceiros, e sim, acredita-se, o estabelecimento de protocolos e procedimentos que tragam algumas garantias nesse contexto.

Shostack e Stewart (2008) afirmam que a práxis do mercado de segurança da informação não é tão objetiva quanto deveria. Segundo os autores, na maioria dos casos seguem-se indicações de fabricantes, entendendo que essas indicações são a "melhor escolha". Essas recomendações geralmente resultam em aquisição de algum produto. Obviamente o mercado deve ser "ouvido" na busca por soluções para certos problemas tecnológicos. Contudo, o mercado não deve ser considerado a fonte de informação principal, tampouco a única.

Atualmente o movimento para transparência do Estado torna os dados abertos (9) facilmente publicados na Internet, portanto livres para uso. Promover dados abertos facilita o acompanhamento e o controle sociais dos relacionamentos estabelecidos entre entidades do Estado e sociedade, inclusive pessoas. Todavia, sua existência se torna "uma espada de dois gumes", especialmente porque pessoas mal-intencionadas ou aquelas que dispõem de muitos recursos computacionais para análise de grande volume de dados podem tirar proveito da desatenção para os riscos de engenharia social a que estão sujeitas as entidades legítimas cujos relacionamentos são publicizados. A utilização dos dados abertos para fins de exploração de vulnerabilidades ainda é uma atividade relativamente complexa, principalmente quando os dados não são estruturados. A tendência é que essa complexidade seja cada vez mais dominada e acessível ao grande público. O risco crescente de mau uso de dados abertos é uma razão para realizar essa pesquisa, que evidencia a necessidade de melhor desenvolvimento de consciência situacional pelas entidades que participam de relacionamentos com o Estado.

4.2 Redes de relacionamento de aquisições de bens de informática

Os autores realizaram duas baterias de coleta de dados no Portal da Transparência. Na primeira bateria, após a

execução das cargas de dados, sobre 25 órgãos superiores do Governo Federal, (por exemplo: Presidência da República, Ministério da Educação, Ministério dos Esportes, entre outros, e sobre 314 outros tipos de órgãos, por exemplo: secretarias, institutos, universidades, agências reguladoras, entre outros) foram executadas coletas em registros de aquisições de bens e serviços de informática de 4.275 Unidades Gestoras (UG) do Governo Federal. A coleta ocorreu em grande volume de dados, durante cerca de dois meses de execução de programa de computador, para coleta de dados sobre dois meses de aquisições públicas. Foram coletados 275 registros de aquisições relacionadas a bens de informática.

Com o aprimoramento posterior do programa de computador, na segunda bateria de coleta de dados foram obtidos 6.943 registros de aquisições de bens de informática do Portal da Transparência. Foram selecionados apenas os registros que continham aquisições realizadas no mês de janeiro de 2014. Foram 122 registros, e essa rede é apresentada na Figura 6. A partir deste ponto foi iniciada a análise de dados.

A Figura 6 ilustra a quantidade de dados, os atores e relacionamentos obtidos com um mês de aquisições de bens de informática. A rede foi criada após todo o processo de coleta de dados já descritos, e é apresentada usando um layout circular.

4.3 Identificação de tríades

Com base na rede ilustrada na Figura 6, foram utilizados ferramentas e métodos de ARS, para a obtenção das tríades incompletas de relacionamentos entre organizações. Após um conjunto de transformações diversas na rede, de classificações, de extrações, de organizações e outras técnicas de ARS, foram obtidas 15 tríades incompletas, onde 4 (quatro) delas são apresentadas nas figuras 9, figura 10, figura 11 e figura 12.

Na tríade presente na Figura 7 observa-se a possibilidade de exploração do papel de corretor intinerante do fluxo de informação por parte do atacante, personificando a empresa RGN – som eletrônica e informática LTDA, em comunicação com os órgãos Polícia Militar do DF e Agência Nacional de Transpores Aquaviários, podendo ser obtidas informação dos dois órgãos públicos em um ataque de engenharia social.

À medida que esse relacionamento presente na Figura 7 fosse aprofundado, estabelecer-se-ia confiança por meio da comunicação, o que poderia proporcionar ao engenheiro social informação sobre os jargões das empresas e as práticas de trabalho. Essas informações são valiosas e poderiam auxiliar no estabelecimento de um elo entre o engenheiro social e as partes, uma vez que este identificaria vulnerabilidades nas relações entre as partes, podendo explorá-las.

Pode-se observar um caso similar de corretor intinerante das informações, ilustrado na Figura 8, onde o Estado-Maior das Forças Armadas adquire bens de informática de duas empresas de um mesmo contexto – contratações de informática. Nesse caso, o engenheiro social poderia por e-mail ou por telefone iniciar uma relação com a empresa Acesso Comércio e Serviço de Informática Ltda. e com a empresa Arte Informática Ltda., possivelmente utilizando uma falsa autoridade do Estado Maior a fim de realizar um ataque. A Figura 9 ilustra um caso similar ao anterior, porém com a Casa da Moeda do Brasil.

Em outro caso, ilustrado na Figura 10, observa-se a possibilidade de personificação da Nuclebras Equipamentos Pesados S/A através do papel de conector das informações entre as empresas de serviços de informática e equipamentos de rede de informática. Poderia supor que as empresas possuem finalidades distintas e, portanto, participam de grupos distintos. Nesse caso, o atacante pode atuar na personificação de qualquer dos órgãos dessa rede social, porém o papel de conector e suas características podem ser explorados apenas na personificação da Nuclebras Equipamentos Pesados S/A.

Utilizar os conceitos de papéis de corretagem – coordenador, corretor itinerante, representante, porteiro, ligador ou conector – para identificação de possíveis alvos de ataques para manipular as pessoas parece simples – um engenheiro social poderia utilizar informações e se valer dos papeis sociais de corretagem para explorar o altruísmo das pessoas, explorar o abuso da confiança. Claro que o ataque em si exige mais passos que a pura identificação do alvo. Existem diversos casos emblemáticos de utilização de ataques de engenharia social (10) com efeitos danosos às organizações respeitadas no mundo (Tabela I). O assunto é mais bem debatido na seção seguinte.

5. Discussão

A pesquisa encontrou alguns aspectos objetivos nas relações de confiança e riscos no contexto da segurança da informação. Para tanto, procurou-se responder à seguinte pergunta: como podem ser identificados os alvos para 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?

Pelo exposto inferimos que nesse cenário caótico e complexo se buscam novas soluções para problemas cotidianos da segurança da informação, e o que se levava como premissa em segurança no passado provavelmente pode ser usado hoje, porém em uma nova visão tecnológica. Entretanto, é importante o

desenvolvimento de pesquisas que possam contribuir para uma melhor percepção da realidade, em uma constante evolução, e não puramente da tecnologia, para que a sociedade possa aprimorar suas relações.

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

O mapa conceitual da Figura 11 apresenta uma visão holística do inter-relacionamento dos conceitos ora estudados. Informação, Confiança, Segurança da Informação, Engenharia Social, Análise de Redes Sociais, entre outros, são inter-relacionados para reforçar o caráter interdisciplinar do campo de estudo da confiança na segurança da informação.

A associação entre segurança da informação e confiança se dá por meio da autorização. A autorização está presente nas três características básicas da segurança da informação, modelada na figura 12, pode-se propor.

A => C, então **C** é ponto fundamental em SI.

Ou seja, sendo **C** a confiança e **A** a autorização, pode-se estabelecer que autorização implica confiança, pois acredita-se que autorizamos quem confiamos. Outrossim, como não é possível prever todas as ações dos autorizados, pode-se concluir que sempre haverá confiança nas autorizações, logo ela é ponto fundamental da SI. Desse modo, sempre haverá risco nas autorizações, pois confiança implica risco. Por conseguinte, fortalece-se a afirmação de alguns autores de que a querela principal da SI é a gestão dos riscos. Por que não minimizar os riscos realizando o controle da confiança interpessoal estabelecida?

Ademais, há um embate entre a importância dos aspectos objetivos e dos aspectos subjetivos para a solução de problemas nesse tema. Alguns defendem que os problemas de segurança podem ser resolvidos puramente com matemática. Outros apregoam que o subjeito é o "elo mais fraco". Portanto, estudar os aspectos subjetivos seria a solução. Além disso, alguns conceitos inerentes a essa problemática, por exemplo a informação, não possuem uma definição unificada, o que dificulta a criação de mecanismos objetivos.

Observa-se que a confiança é um aspecto presente em uma nova dimensão da segurança da informação e em todos os momentos no contexto organizacional. Se a base para a segurança da informação é firmada em seus aspectos fundamentais de confidencialidade, integridade e disponibilidade, a confiança surge como um elemento integrante e gera uma nova dimensão, influenciando todos os elementos bases da segurança da informação (Figura 13).

A confiança, para Schneier (2012), pode ser construída 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. Os autores entendem que a confiança é um elemento fundamental para a sociedade, e quanto mais algo é importante para a coletividade, maior é a probabilidade de ele ser atacado. Entende-se que a autenticidade deve ser uma preocupação constante para evitar o fenômeno da personificação e promover autorizações mais seguras.

Na conjuntura desse estudo, a confiança é um fenômeno social e pode ser observada com ARS. Pode-se afirmar que nas organizações existem espaços de comunicação e relacionamentos expressos e interdependentes que, consequentemente, estão dotados de manifestações de confiança. Se a ARS estuda o fluxo de informações e relacionamentos interpessoais, deduz-se que ela pode ser usada para se estudar o fenômeno da confiança, consoante afirmou Everton (2013), tendo em vista que a confiança é desenvolvida com base nas comunicações e nos relacionamentos interpessoais, segundo Swan et al. (2001) e seus colaboradores. Ora, se a comunicação organizacional é formada pelo fluxo de mensagens em uma rede de relacionamentos, não é tolice pensar que a confiança se manifesta no cenário do fluxo da informação e pode ser observada utilizando-se a ARS.

De forma prática o método de coleta e análise de dados, e a validação da argumentação obtida com o levantamento, demonstram que é possível selecionar alvos potenciais para ataques com o tratamento de dados no Portal da Transparência do Governo Federal. Se o contexto é propício ao ataque, possivelmente os alvos serão explorados, a menos que esses alvos tenham consciência situacional apropriadamente desenvolvida. Os modelos de comportamento obrigatório dos alvos devem ser ajustados constantemente para aprimorar as condutas dentro do contexto, especialmente ligadas à garantia de autenticidade nas comunicações da informação sobre meios digitais. Isso é, o fortalecimento do controle sobre a autenticidade das relações sociais deve ser consequência do desenvolvimento dessa consciência situacional sobre os riscos de exploração da confiança em comunicações digitais.

Souza (2011) afirma que a confiança é um componente estratégico no contexto da segurança da informação. Schneier (2012), por sua vez, considera a segurança um mecanismo para amparar uma conjuntura de confiança favorável ao desenvolvimento social em grande escala.

Os modelos de comportamento obrigatório de Reale combinados com o que ensina Schneier (2012) agem como pressões sociais para criar mecanismos de confiabilidade.

A informação é o objeto a se proteger na segurança da informação. É preciso tomar certos cuidados a quem confiamos a informação. Além dos trabalhos de prevenção para confiar adequadamente, também é preciso ter controle dinâmico sobre as relações de confiança estabelecidas para poder revogar determinadas autorizações, arriscadas demais, por exemplo, passíveis de engenharia social.

A segurança da informação é um processo, e não um produto (Schneier, 1998). Souza (2011) defende que com controles e contramedidas bem desenhados pode-se garantir a segurança das informações nas relações organizacionais. Por meio de estudos metódicos, com a finalidade de desenvolver esses controles e contramedidas pode-se interromper determinados comportamentos danosos ou maliciosos em um ambiente organizacional.

Percebe-se ser possível sistematizar as abordagens de análise de segurança com o uso da ARS. Entende-se que o controle com o uso de sociogramas é interessante em diversos aspectos da segurança da informação, inclusive na engenharia social, melhorando a visualização de certos problemas e possibilitando melhores insights, o que facilitaria a prevenção de problemas.

Então, foi possível encontrar possíveis alvos para ataques de engenharia social. É claro que o método apresentado não esgota o assunto, mas temos certeza que apresenta uma linha de pensamento e abre o horizonte para novos estudos. Assim, a análise de redes sociais é uma boa ferramenta para explorar e analisar dados de segurança da informação. O assunto é mais bem fundamentado, explorado e discutido na dissertação que deu causa a este artigo.

6. Considerações finais

Existem dificuldades de controle para dados em segurança da informação e segurança cibernética principalmente devido ao ambiente no qual elas estão inseridas, por exemplo, as organizações e a Internet. Portanto, há demanda para novos processos e métodos de análise em segurança da informação sobre dados abertos. Ambientes complexos e caóticos são difíceis de controlar.

É importante dizer que este artigo procura demonstrar a ponta do iceberg no suporte à tomada de decisão em diversos aspectos da segurança da informação governamental com a observação das relações de confiança, auxiliando, talvez, a criação de um arsenal analítico. Por exemplo, o método aqui estudado daria melhor visibilidade sobre o impacto de ações de publicação de informações no contexto da TI em ambientes abertos, como o Portal da Transparência, e outras aplicações. Poderiam ser monitoradas as relações de confiança aos autorizados a acessar certas informações protegidas.

Conclui-se esse trabalho afirmando que a confiança está presente nas comunicações. Ela pode ser percebida por meio da ARS e poderia ser mediada com o uso da observação do fluxo das informações no ambiente informacional. Dessa forma, se a engenharia social pode ser efetuada com o abuso da confiança e a confiança pode ser observada com a ARS, pontos de abuso da confiança podem ser observados com a ARS. Afinal, a sociedade é dinâmica, e por intermédio do monitoramento e da análise pode ser que se consiga entender as mudanças e recomendar ajustes de seus enquadramentos sociais.

Notas

(1) Silva (2006) informa que o termo objetivo é derivado do verbo latino objecere (pôr diante, apresentar); o vocábulo quer exprimir literalmente tudo o que é visível, concreto, real, positivo; oposto à subjetividade, que se refere ao sujeito.

(2) Segundo Fernandes (2012), o termo "cibernética" é resgatado por Wiener em 1948. Fernandes discute o trabalho de Wiener, que apresentou vários ensaios sobre os fenômenos de controle, identificados por meio da análise do comportamento de sistemas mecânicos, sistemas autorreplicantes, sistema nervoso, fenômenos psíquicos, máquinas computacionais, sociedades humanas e animais. Para este autor, a investigação de fenômenos de controle, monitoramento, feedback e autorregulação foi disseminada no trabalho de Wiener, que cunhou o termo "cibernética". Além disso, um fator gerador das ameaças em segurança da informação seria confiar erroneamente em alguém ou em alguma tecnologia da informação no espaço cibernético.

(3) O Pajek é um software esloveno utilizado para a análise de redes sociais.

(4) O hacker, segundo Bill e Klein (2010) quebra as regras que ele julga estúpidas para chegar a resultados que ele considera melhores, mais espertos e mais inteligentes. Schneier (2012) doutrina que o outlier – podemos entender como o hacker – é aquele que não aceita as pressões sociais e age de acordo com seus ideais, seu desejo, sua conveniência e seu egoísmo. Aos olhos do Direito, o hacker é aquele que aponta vulnerabilidades no sistema, enquanto o cracker é o que pratica ações ilícitas

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

(6) 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 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, pois estes nos ajudam a reduzir a complexidade e a suprimir partes para podermos nos concentrar no que realmente interessa (Krogerus e Tschäppeler, 2011).

(7) A personificação ocorre quando um atacante pode introduzir ou substituir uma identidade, induzindo outros a pensarem que essa identidade falsa, ao invés da legítima, é a correta. Dessa forma, o atacante se passa por outro indivíduo.

(8) A regra de necessidade de saber trata-se da norma que determina que as informações serão acessadas apenas por aqueles que necessitam saber daquela informação para executar suas atividades de trabalhos.

(9) O Projeto Dados Abertos (do inglês Project Open Data) está registrado no creative commons. O Open Data (2013) afirma que "dados abertos são aqueles livres para serem utilizados, reutilizados e redistribuídos por qualquer um, sem restrição (exceto, talvez, os requisitos de propriedade e compartilhamento)" (tradução nossa).

(10) No escritório da RSA, por meio da engenharia social foi possível ultrapassar o perímetro de acesso a informações internas do escritório e por meio do escalonamento de privilégios foram acessadas informações classificadas. Esse ataque deu origem a diversos outras ataques a correntistas de banco que utilizavam a ferramenta SecureID token (Watson et al., 2014).

Referências

Bill, J.; Klein, J. (2010). Hacking Work: Breaking Stupid Rules for Smart Results. London, England: Penguin Books Ltd, 2010.

Castelfranchi, C.; Falcone, R. (2001) Social Trust: A Cognitive Approach. Unit of AI, Cognitive Modelling and Interaction. Roma, Italy: National Research Council - Institute of Psychology. 2001.

Chiavenato, I. (2003). Introdução à teroria geral da administração: uma visão abrangente da moderna administração das organizações. Rio de Janeiro: Elsevier, 2003.

Command Five Pty Ltd. (2011). Advanced Persistent Threats: A Dacede in Review. [S.l.]: Command Five Pty Ltd., 2011, p. 1-13.

De Nooy, W.; Mrvar, A.; Batagelj, V. (2011). Exploratory Social Network Analysis with Pajek: Structural Analysis in the Social Sciences. 2. ed. New York: Cambridge University Press, 2011.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. // Human Factors 37:1 (1995) 32–67.

Everton, S.F. (2013). Disrupting Dark Networks (Structural Analysis in the Social Sciences). New York: Cambridge University Press, 2013.

Fernandes, J.H.C. (2010). Segurança da Informação: Nova Disciplina na Ciência da Informação? // XI Encontro Nacional de Pesquisa em Ciência da Informação. Rio de Janeiro: [s.n.], 2010.

Fernandes, J.H.C. (2012). 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.

Hill, C.A.; O'Hara, E.A.A (2005). Cognitive Theory of Trust. Twin Cities. Minnesota: University of Minnesota, 2005.

Krogerus, M.; Tschäppeler, R. (2011). El Libro de las decisiones, 50 modelos de éxito: Pequeño manual de decisiones estratégicas. Buenos Aires: Pluma y Papel, 2011.

Lazarte, L. (2000). Ecologia cognitiva na sociedade da informação. Brasília - DF: Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), 2000.

Mäkinen, H. (2005). Risk, Trust and Security. Knowledge of Society White Pape, Ann Arbor, Michigan, USA, 2005. www.YhteiskunnanTieto.fi.

Mitnick, K.; Simon, W.L. (2002). The art of Deception: Controlling the Human Element of Security. Indianapolis, Indiana: Wiley Publishing, Inc., 2002.

Open Data Commons (2013). Making Your Data Open: A Guide, Open. opendatacommons.org, 2013. http://opendatacommons.org/guide/#sthash.K28tpib6.dpuf (16-08-13.

Reale, M. (2000). Lições preliminares de direito. 25. ed. São Paulo: Saraiva, 2000.

Ressler, S. (2006). Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. Homeland Security Affairs, Sunderland, UK, v. II, n. 2, Jul 2006. www.hsaj.org.

Rezende, P.A.D. (2011). Modelos de confiança para segurança em informática. Brasília. [S.l.]: Universidade de Brasília (UnB), 2011.

Saracevic, Tefko. (1995). Interdisciplinary nature of information science. Ciência da Informação, v. 24, n. 1, 1995.

Schneier, B. (1998). Secrets and Lies: The Myth of Security in the Digital World. [S.l.]: John Wiley & Sons, 1998.

Schneier, B. Liars and Outliers: Enabling the Trust that Society needs to Thrive. Indianapolis: John Wiley & Sons, Inc., 2012.

Shostack, A.; Stewart, A.A (2008). Nova Escola da Segurança da Informação. Rio de Janeiro: Alta Books, 2008.

Silva, Antonio Braz de Oliveira E; Matheus, Renato Fabiano; Parreiras, Fernando Silva; Parreiras, Tatiane A. Silva. (2005). Análise de Redes Sociais como metodologia de apoio para a discussão da interdisciplinaridade na Ciência da Informação. Belo Horizonte: [s.n.], 2005.

Silva, D.P.E. (2006). Vocabulário Jurídico. 26. ed. Rio de Janeiro: Forense, 2006.

Souza, R.C.D. (2011). 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, William; Cooper, Rachel; McDermott Rachel; Wood, Graham (2001). A Review of Social Network Analysis for IMI Trust in Construction Project. 17th Annual ARCOM Conference. Salford: Association of Researchers in Construction Management, 2001, p. 59-67.

Wassermann, S.; Faust, K. (1994). Social Network Analysis: Methods and Applications. 8. ed. New York: Cambridge University Press, 1994.

Watson, G.; Mason, A.; Ackroyd, R. (2014). Social Engineering Penetration Testing: Executing social engineering pen tests, assessment and defense. Oxford, UK: Elsevier, 2014.

Wolff, K.H. (1950). The Sociology of George Simmel. Illinois: The Free Press, 1950.

Received: 2015-06-17. Accepted: 2016-02-24

Apêndice

No apêndice encontra-se as figuras do artigo.

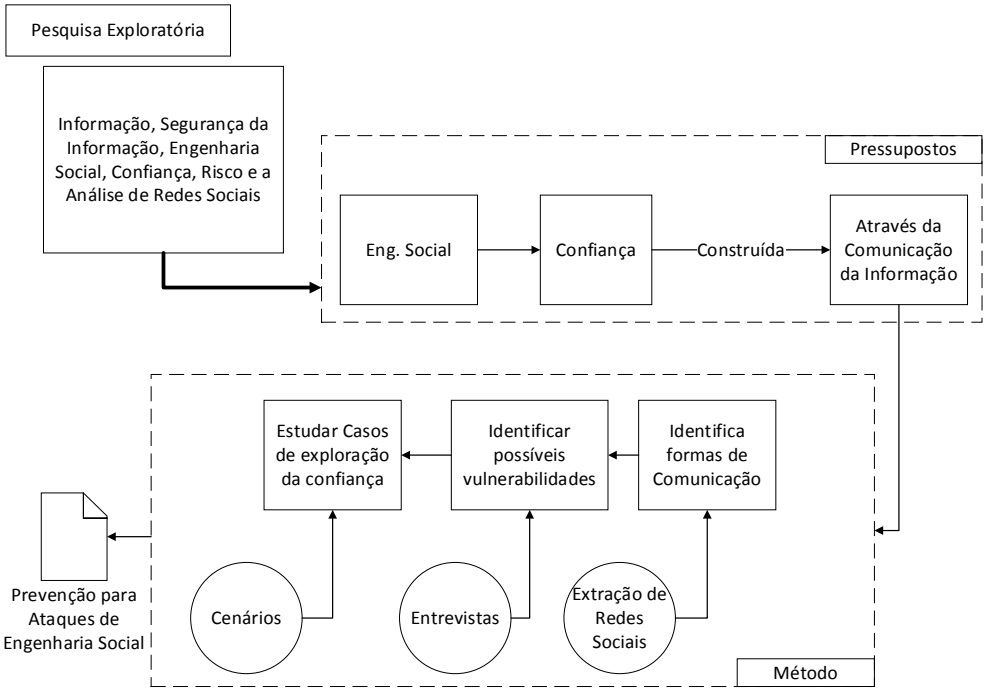

Figura 1. *Processo metodológico*.

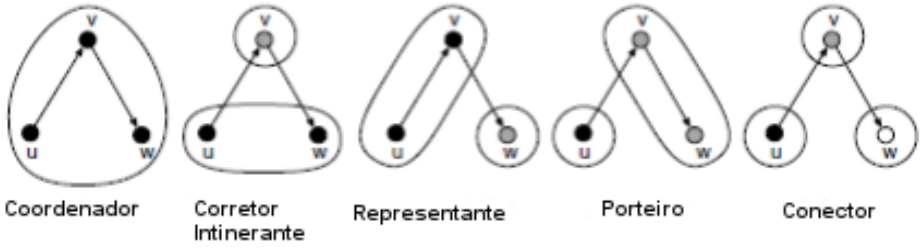

Figura 1. *Papéis de corretagem em uma rede social Fonte: De Nooy et al. (2011)*

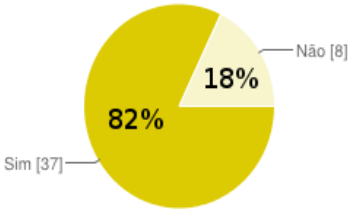

Figura 2. *Fração de consultados que recebem afazeres por mensagem remota*

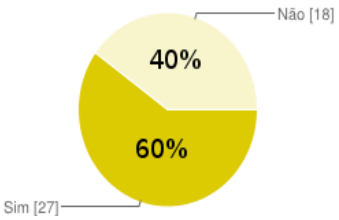

Figura 3. *Fração de consultados que receberam ou enviam senhas por mensagem remota*

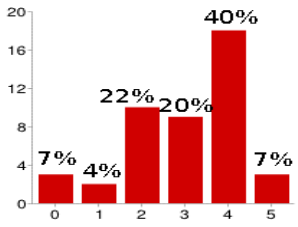

Figura 4. Escala de confiança do consultados nos fornecedores

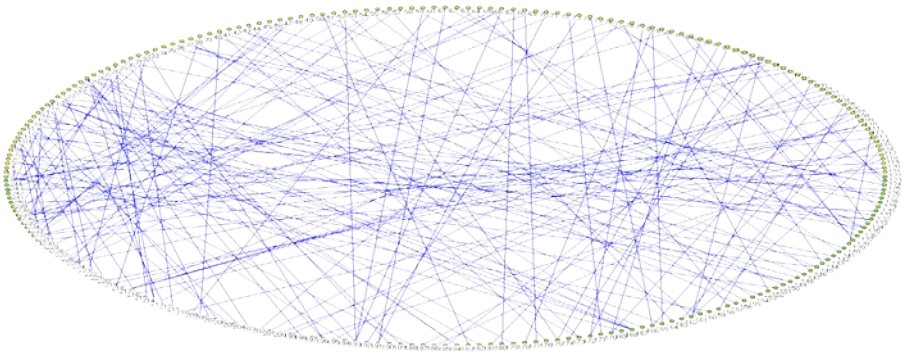

Figura 5. *Sociograma da rede que associa cliente e fornecedor de bens de informática.*

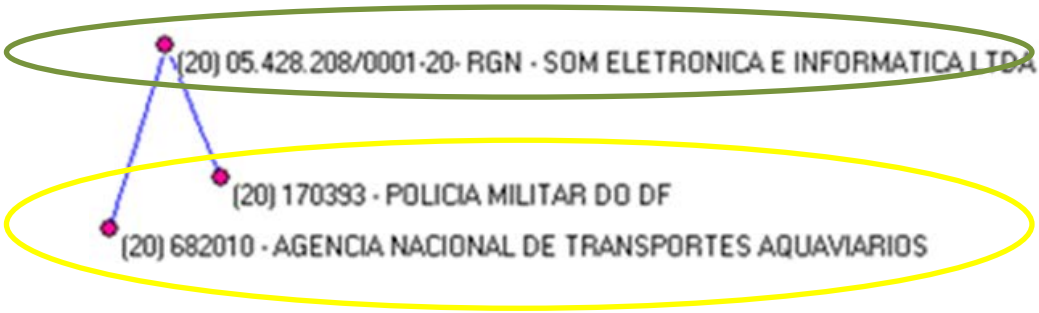

Figura 6. *Uma tríade extraída de rede da figura 6: dois entes públicos adquirem de um mesmo fornecedor*

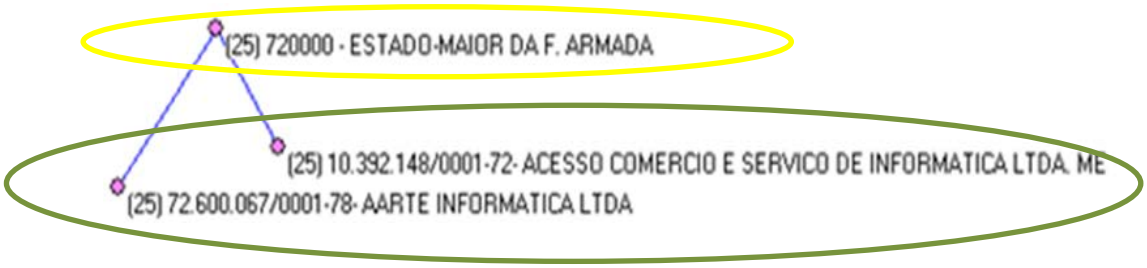

Figura 7. *Uma tríade incompleta extraída da rede da figura 6: Um ente público adquire de dois fornecedores distintos*

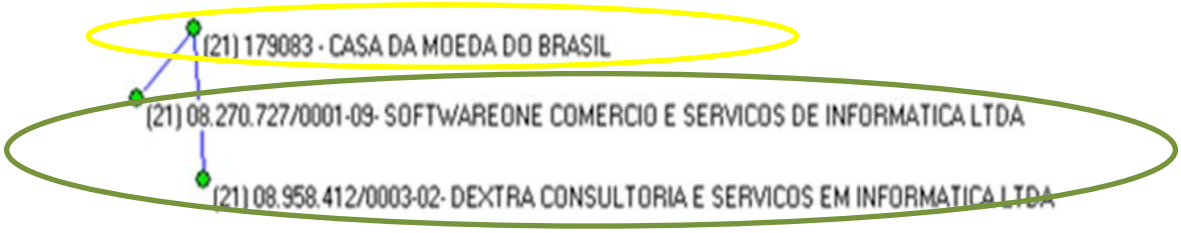

Figura 8. *Outra tríade extraída da rede da figura 6: uma empresa pública adquire de dois fornecedores privados*

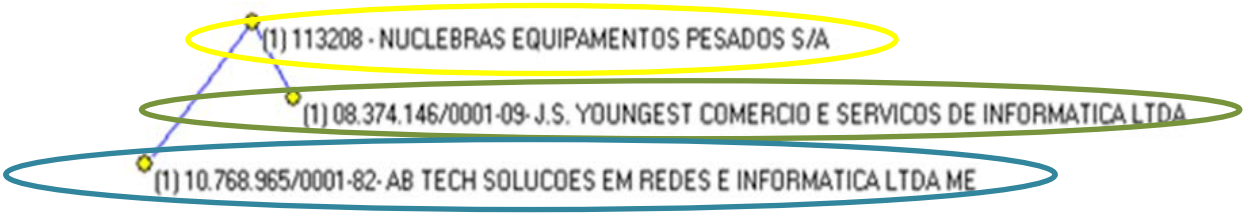

Figura 9. *Uma tríade incompleta extraída da rede da figura 6: uma empresa pública adquire serviço e equipamentos de rede*

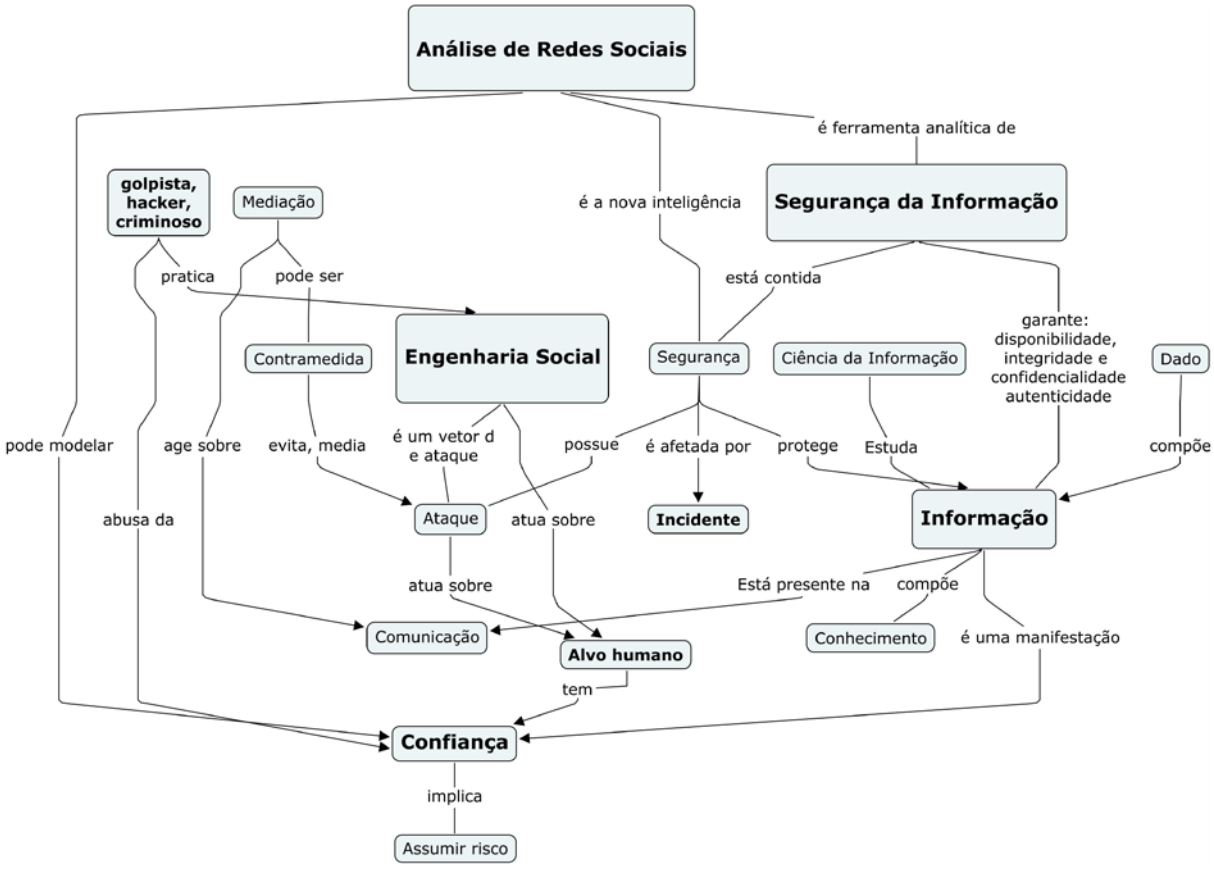

Figura 10. *Mapa conceitual da discussão*

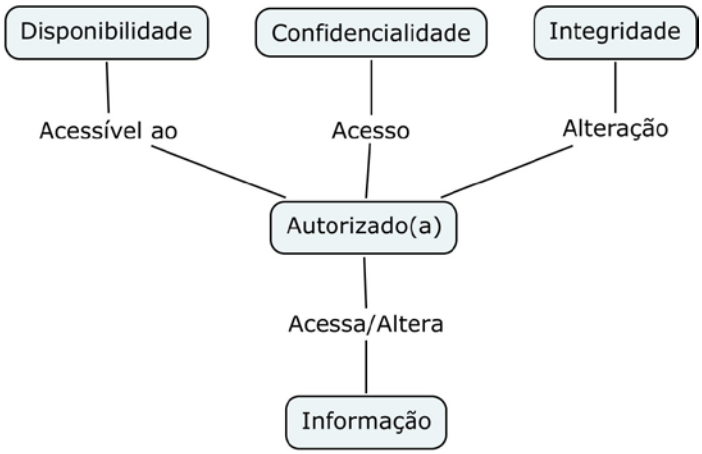

Figura 11. *A confiança está no cerne da SI*

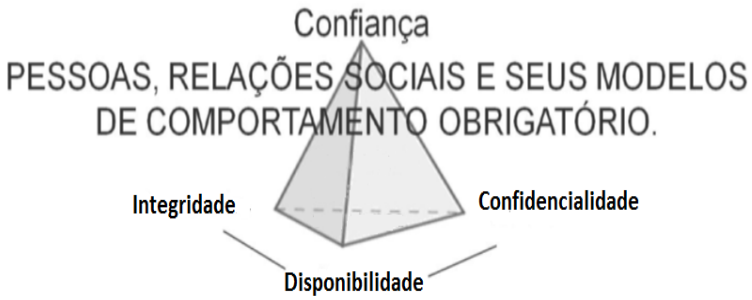

Figura 12. Confiança como elemento essencial da SI