Engenharia social nas redes sociais *online:* um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação

Narjara Bárbara Xavier Silva
narjara.barbara@gmail.com
Universidade Federal da Paraíba

Wagner Junqueira de Araújo
wagnerjunqueira.araujo@gmail.com
Universidade Federal da Paraíba

Patrícia Morais de Azevedo
patriciamoraisrp@gmail.com
Universidade Federal da Paraíba

Resumo: O desenvolvimento dos sites de redes sociais (SRS) fez surgir o fenômeno conhecido como "hipermobilidade estética dos internautas" que aumenta a exposição de informações pessoais na Web, aumentando também os riscos associados a estas, principalmente em relação à aplicação de técnicas de engenharia social. A engenharia social é um termo que define algumas práticas utilizadas para obter acesso a informações, por meio da quebra de sigilo em sistemas, organizações ou de indivíduos, utilizando-se de pesquisas, trapaças, ou exploração da confiança das pessoas. Diante deste cenário, como mensurar quanto as informações de determinado indivíduo estão expostas na Web? Para responder tal questão, este trabalho teve como objetivo analisar o grau de exposição de informações de pessoas físicas acessíveis na Web. Para tanto, esta pesquisa foi desenvolvida como um estudo de caso, com abordagem quantitativa e qualitativa, com foco no levantamento de informações pessoais e profissionais, utilizando-se de consultas a sites e portais de acesso livre na Web. Foi utilizada a amostragem do tipo não probabilística e elaborada uma métrica em escala para classificação do grau de exposição. Da amostra, 70% apresentam um indicador de exposição alta e 20% extremamente alta em relação às informações levantadas. Nenhum dos indivíduos pesquisados apresentou zero ou baixo grau de exposição. A partir desse estudo foi possível demonstrar a facilidade na busca e encontro de informações referentes a um determinado usuário no ambiente *online* e que são suficientes para subsidiar ataques de engenharia social. Os resultados obtidos permitem criar hipóteses que podem ser trabalhadas em uma pesquisa com amostra probabilística e ressalta a necessidade da adoção de procedimentos de gestão da segurança da informação e implantação de políticas de segurança da informação no ambiente organizacional e para uso pessoal.

Palavras-chave: gestão da informação e do conhecimento; gestão da segurança da informação; redes sociais; engenharia social; informação pessoal.

Abstract: The development of social networking sites (SNS) has created a phenomenon known as "hyper mobility esthetics of netizens" that increases of the exhibition of personal information on the Web, it is natural that raises the risks associated with such, especially relative to the application of social engineering techniques. Social engineering is a term that defines some practices used to get access to information, through the breaking systems confidentiality, organizations or individuals, using surveys, cheating or exploiting the trust of people. Faced this scenario, how measure the private information of a particular individual are exposed on the Web? To answer this question, this study aimed to analyze the degree of exposure of information is accessible on the Web. To this end, this research was conducted as a case study with quantitative and qualitative approach, focusing on survey personal and professional information, using consultations to sites and open access Websites. It was used the non-probabilistic sampling and elaborates a metric scale for rating the degree of exposure. We observed that 70% of the samples have a high exposure indicator and 20% extremely high. No individuals surveyed had zero degree of exposure. From this study was possible to demonstrate the facility in searching and gathering information in the online environment. This information is sufficient to subsidize a social engineering

attacks. The results obtained allow us to create hypotheses that can be worked on a research of a probabilistic sample and highlight the need to adapt procedures for information security management and implementation of information security policies in the organizational environment.

Keywords: information and knowledge management; information security management; social networks; social engineering; personal information.

1 INTRODUÇÃO

Com base na obra "O livro dos códigos", de Simon Singh (2001), observa-se que desde o antigo Egito a informação é vista como elemento de valor, cuja importância se revela segundo os interesses culturais, políticos e econômicos da sociedade. Observa-se, assim, a existência e a evolução de uma "batalha intelectual" entre os criadores de códigos e os decifradores, ou seja, de um lado o emissor que transmite a mensagem em códigos, quando aplicável, para que ela possa chegar de forma segura ao seu receptor - povos, governos, pessoas ou organizações, e do outro, os decifradores, que buscam decodificar as mensagens a fim de obter vantagem da informação decodificada, seja para fins militares, pessoais ou para corporativos.

Na sociedade da informação, a partir da industrialização e do aumento da competitividade empresarial, a informação passou a ser considerada como elemento essencial à formação da inteligência competitiva, sendo utilizada cada vez mais de forma estratégica para a tomada de decisão e otimização dos resultados. Porém, "ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes" (BRASIL, 2003, p. 9). Isso porque, diferente da sociedade clássica ou pré-informacional, na sociedade da informação, com a difusão da Internet e o desenvolvimento das Tecnologias da Informação e Comunicação (TIC), as empresas se utilizam cada vez mais da rede mundial de computadores como principal canal para geração de negócios, ampliando, dessa forma, a possibilidade de incidentes no ciclo de vida da informação (criação, manuseio, armazenamento, transporte e descarte), podendo comprometer os resultados organizacionais.

Nesse contexto, faz-se necessária a abordagem estratégica à gestão de segurança da informação, considerada como um "diferencial determinante na competitividade das corporações" (PROMON, 2005, p. 3) e conceituada como uma "área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade" (PEIXOTO, 2006, p. 37). Como complemento a essa definição conceitual, Sêmola (2006) indica que para conferir um

tratamento de segurança a uma informação de forma eficiente, é necessário garantir suas principais propriedades. A saber:

> (1) confidencialidade – acessibilidade da informação aos agentes autorizados e inacessibilidade aos agentes não autorizados; (2) integridade – possibilidade de alteração da informação para os agentes autorizados e impedimento de alteração para os agentes não autorizados; e (3) disponibilidade – acessibilidade da informação apenas aos agentes autorizados a qualquer momento. (SEMOLA, 2006)

Para o autor, essas propriedades estão relacionadas às variáveis organizacionais que são de competência da fase do diagnóstico do ambiente informacional, revelando, dessa forma, os problemas de segurança da informação e contribuindo para o levantamento das ações de tratamento da informação para a antecipação de incidentes e planejamento de soluções. Essas variáveis são identificadas ainda por Sêmola (2006) como componentes de risco em segurança da informação. São eles: a) ameaças – podendo ser internas (ex.: desastres naturais, como inundação; ação voluntária por funcionários insatisfeitos, ou ação involuntária por ingenuidade) e externas (*cracker*, engenharia social, vírus); b) vulnerabilidades – considerando as principais como físicas (ex.: ausência de mecanismo de controle de acesso); tecnológicas (ex.: configuração inadequada de *firewall* ou de projetos de *software)* ou humanas (ex.: ausência de conscientização por meio de treinamentos para disseminação de políticas de segurança da informação; e c) impactos – resultado de um incidente indesejável (ex.: prejuízo financeiro; danos à imagem).

A partir das propriedades da informação e suas vulnerabilidades, o fator humano é considerado o elemento mais importante na gestão de segurança da informação, como também é o elo mais fraco da segurança (MITNICK; SIMON, 1963), pois são as pessoas que executam e suportam os processos de uma organização. Ainda segundo os autores, “a segurança não é um problema para a tecnologia – ela é um problema para as pessoas e a direção” (MITNICK; SIMON, 1963, p. 4).

Não adianta a organização investir em sistematização de processos e implementação de tecnologias sofisticadas se os seus funcionários estão insatisfeitos, podendo utilizar informações corporativas de forma intencional e indevida, ou se não estão conscientes das ameaças existentes através do relacionamento interpessoal e da comunicação humana dentro e fora da organização, possibilitando o repasse de informações sigilosas de forma involuntária a pessoas mal intencionadas por meio da engenharia social – técnica considerada como a maior ameaça à segurança da informação nas organizações, por meio da persuasão, manipulação e influência das pessoas, a fim de obter informações sigilosas (MITNICK; SIMON, 1963).

Nesse contexto, faz-se necessário, o direcionamento da atenção das organizações aos tipos, meios e técnicas de engenharia social, utilizados para ataques à confidencialidade,

integridade e disponibilidade das informações no âmbito organizacional, pois, como afirmam Mitnick e Simon (1963, p. 4), “os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas”.

Dessa forma, a quebra de segurança da informação, a partir das vulnerabilidades humanas, se torna cada vez mais frequente devido ao baixo custo para implementação dos ataques, pois basta um computador com acesso a internet, associado ao baixo risco na identificação do atacante, então chamado de engenheiro social – o profissional da “arte de enganar” (MITNICK; SIMON, 1963).

2 ENGENHARIA SOCIAL

Com base nas abordagens de Mitnick e Simon (1963) e Guilherme Júnior (2006), a engenharia social podemos definir como um conjunto de práticas utilizadas para a obtenção de informações relevantes ou sigilosas de uma organização ou indivíduo, por meio da persuasão, manipulação e influência das pessoas, seja com o uso ou não da tecnologia. Corroborando essa conceituação, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (2012, p. 115) define engenharia social como “uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações”, podendo ser de uso benéfico ou não, protegendo ou atacando um sistema de segurança de informação empresarial ou até mesmo particular.

Em relação à atividade profissional, o engenheiro social não possui uma formação definida; ele pode atuar em qualquer área, entretanto, seu foco de atuação são empresas de médio e grande porte. Os engenheiros sociais aplicam técnicas como uma boa conversa e simpatia, analisam o ambiente e, principalmente, suas futuras vítimas, identificando seus pontos fracos e as vulnerabilidades do ambiente visado. A partir daí iniciam seu ataque. Na análise dessas vulnerabilidades, as relacionadas ao ser humano são consideradas o principal fator de ataques do engenheiro social. Dentre elas, Guilherme Júnior (2006) destaca como as mais relevantes: a) vontade de ser útil – tratamento com cortesia; b) busca por novas amizades – ampliação da rede de relacionamentos; c) propagação de responsabilidades – compartilhamento de funções e atividades; e d) persuasão – características comportamentais que tornam as pessoas vulneráveis à manipulação por meio de conversas informais.

Diante destas características, qualquer pessoa pode se tornar um engenheiro social, manipular pessoas e obter informações sigilosas a fim de interferir em qualquer tipo de negócios. Tanto os *hackers* (pessoas que invadem os sistemas de computadores sem interesses financeiros, somente pelo desafio), como *crackers* (indivíduos que invadem com intuído de destruir, roubar dinheiro, senhas ou informações), podem se valer das técnicas de engenharia

social, são pessoas com diferentes perfis, como estudantes, representantes comerciais, executivos, ex-funcionários, vigaristas, terroristas etc. Após a identificação das vulnerabilidades existentes no âmbito das pessoas e do ambiente que o engenheiro social pretende atacar, deve-se entender como se dá o processo em si de interferência e ataque. De forma sucinta, o engenheiro social percorre as seguintes etapas: 1) reúne todo tipo possível de informações sobre as pessoas, seus perfis, vulnerabilidades relacionadas e as do ambiente; 2) desenvolve relacionamento com a vítima por meio da aproximação e estreitamento de laços, a fim de ganhar confiança e obter acesso aos dados e ambientes; 3) explora todo tipo possível de informação e relacionamento na área de ataque; e 4) executa o ataque à empresa ou ao indivíduo (LENNERT e OLIVEIRA, 2011).

Para esta última etapa, conforme Lennert e Oliveira (2011), o engenheiro social faz uso das mais diversas técnicas, tais como: a) *phishing* – invade computadores por meio de vírus e busca as informações de interesse; b) abordagem física – faz chamadas por telefone buscando informações precisas para uso indevido, recolhe documentos e papéis de conteúdo relevante que não foram devidamente descartados, por exemplo, no lixo; c) abordagem psicológica – usa do apelo sentimental e da amizade; d) entretenimento – faz uso das conversas em locais de lazer , quando o indivíduo está distraído, para obter informações de seu interesse e, por fim, e) solidariedade – faz uso da generosidade das pessoas desenvolvendo, por exemplo, campanhas de doação e eventos restritos.

O que se observa é que, com o desenvolvimento dos sites de redes sociais (SRS), as vulnerabilidades de caráter humano são potencializadas pelo fenômeno conhecido como “hipermobilidade estética dos internautas” (STASSUN; ASSMANN, 2012). Para os autores, esse fenômeno é caracterizado pela necessidade de o sujeito se sentir importante por meio do (re)conhecimento e aparência com que se revela nos SRS, por meio de suas informações e intimidade expostas de forma intencional e espetacularizada. Dessa forma, o ambiente *online* é identificado como um dos nichos de atuação dos engenheiros sociais, devido à grande acessibilidade, exposição, instantaneidade e a falhas de gestão da segurança da informação, conforme abordado a partir do próximo tópico.

2.1 Engenharia Social nas Redes Sociais Online

A necessidade humana de socialização e interação através da aglomeração em grupos/redes não é recente. Porém, com o desenvolvimento da Internet, os SRS nascem com o objetivo de atender de forma otimizada essa necessidade, gerando oportunidades para novas formas de interação e relacionamento entre os indivíduos no ambiente virtual. Nessa perspectiva, Recuero (2009, p. 102) afirma que SRS “são espaços utilizados para expressão das redes sociais na Internet”. As redes sociais, por sua vez, são definidas como um conjunto de

dois elementos: atores sociais e suas conexões. Segundo Boyd e Ellison (2007), os SRS são serviços que permitem aos indivíduos: (1) construir um perfil público ou semi-público dentro de um sistema limitado; (2) articular-se com uma lista de outros usuários com os quais se compartilhará uma conexão; (3) ver e percorrer a sua lista de ligações e aquelas feitas por outras pessoas dentro do sistema.

Em concordância com Cavalcanti Junior (2011), hoje os sites de redes sociais, com foco no relacionamento, podem ser caracterizados como o conjunto de ferramentas com maior facilidade para fazer amigos, manter contatos e conhecer pessoas por meio da Internet. Porém, também podem ser caracterizados como uma grande ameaça à privacidade dos seus usuários, pois esses sites possuem/expõem um grande volume de informações pessoais e/ou profissionais, incluindo o ciclo de amizades, fotos, lugares que frequentam, endereço residencial e números de contato, cargo e emprego atual, e ainda, os familiares, aumentando o nível de visibilidade na Internet e as possibilidades de ataques de engenharia Social.

No âmbito organizacional, essas ameaças passam de um plano individual/pessoal para um plano corporativo/mercadológico, pois os SRS podem ser utilizados pelo engenheiro social para obter informações sigilosas sobre a empresa, seja através de pessoas identificadas e mal intencionadas que se tornam "amigas" apenas para este fim, tais como usuários se fazendo passar por um profissional da empresa, ou até mesmo através de perfis falsos, os chamados "*fakes*". Essas ameaças se agravam pelo fato de muitas empresas permitirem o acesso a redes sociais no ambiente corporativo, como também muitas pessoas aceitarem o pedido de "amizade" de usuários nesses sites mesmo sem conhecer os seus autores.

Segundo estudos publicados pelo porta G1 (2012), somente em 2012, os crimes virtuais causaram um prejuízo de R$ 15,9 bilhões no Brasil, atingindo 28,3 milhões de pessoas. Entre os crimes relacionados estão: o uso de *Internet banking,* vírus, furto de dados pessoais, invasão de e-mails e perfis sociais, invasão de dispositivos móveis e *bullying online*. A pesquisa aponta ainda um aumento no número de crimes *online* em plataformas móveis e sociais com relação aos anos anteriores. Conforme os dados, 15% dos usuários de redes sociais relatam ter sofrido de invasão de perfil e uso de identidade de forma indevida. Ainda segundo a pesquisa, um em cada dez usuários de redes sociais foi vítima de golpe ou links falsos em plataformas colaborativas.

Esse aumento no número de crimes cibernéticos pode ser justificado pelo aumento do número de usuários na Internet, que, segundo indicadores (2012) da Safernet, chegam a 81.798.000 de pessoas no Brasil. Desse total, pelo menos 87,6% dos internautas estão em algum tipo de sites de relacionamento, segundo dados apresentados por Damasceno (2012), classificando o Brasil em primeiro lugar no ranking mundial de adesão às redes sociais. Ainda, segundo estatísticas da Social Bakers (2012), referente ao ano de 2012, 63.161.560 desses

usuários possuem perfil no SRS Facebook, classificando o país em segundo lugar no ranking mundial de estatísticas desse ambiente.

Fazendo um levantamento mais específico quanto ao uso do Facebook, Furlan (2012) reuniu estatísticas sobre esse SRS. Segundo dados referentes ao mês de abril de 2012, o Facebook no Brasil recebeu 9,76% de todas as visitas da Internet; 1 em cada 4 páginas visitadas por um único usuário pertenciam às redes sociais. Já em relação ao ano de 2011, no Brasil, o termo "Facebook" foi o mais buscado na Internet. Diante desses dados é possível inferir o aumento na visibilidade dos usuários nos SRS e os tipos de ameaças relacionados ao uso desses sites.

O Facebook é aberto para qualquer pessoa que tiver interesse em se cadastrar. Para isso, basta acessar o site e preencher as informações solicitadas para criação de perfil. Dentre as informações necessárias à criação de um perfil completo estão: lugar onde o usuário trabalha/trabalhou; lugar onde estuda/estudou; cidade onde nasceu e onde mora; data de aniversário; status de relacionamento, caracterizado como solteira (o), noiva (o), casada (o), em um relacionamento enrolado, em um relacionamento aberto, viúva (o), separada (o), divorciada (o); interesses (opção sexual, religião e preferência política); e endereço e contatos (celular, telefone, e-mail, sites, outras redes).

Após a criação do perfil, os usuários podem fazer "solicitações de amizade" para se conectarem a outras pessoas. Além disso, podem identificar pessoas da sua família de acordo com o tipo de parentesco (ex: mãe, pai, primo (a), tio (a)). Outra forma de organizar os contatos é por meio da criação de grupos/listas, de acordo com o seu círculo de amizades e ainda há a possibilidade de marcar os seus amigos como "melhores amigos", passando a receber as suas atualizações diárias na sua *timeline* (linha do tempo). Uma opção que talvez seja diferente dos outros sites é se tornar "assinante" de seus amigos para receber o *feed* de notícias. Essa opção também pode ser escolhida para pessoas "não amigas". Ou seja, as suas postagens marcadas como públicas serão visíveis na *timeline* do usuário que se tornou assinante do seu perfil. Quanto a essa opção, o usuário ainda pode escolher receber "notificações do assinante" no Facebook, por SMS, notificações no modo *push* (alertas em celular) ou por e-mail.

Dentre as formas de comunicação no Facebook estão: a opção de postar vídeos e fotos, seja em sua *timeline* ou em álbuns separados por temas; criação e gerenciamento de eventos, podendo convidar ou ser convidado pelos usuários; postagem de textos ou comentários pessoais. Quanto às postagens (fotos, textos, vídeos), elas podem ser "curtidas" ou compartilhadas, e ainda possuem a opção de marcar pessoas e lugares. Além dessas ferramentas, o Facebook também possui aplicativos com objetivos específicos que podem ser

utilizados pelo computador com acesso à Internet ou por celular ou tablet, por exemplo: *Instagram* (fotografias), *Foursquare* (geolocalização), e diversos tipos de jogos.

Diante dessas informações que podem ser disponibilizadas pelos usuários a suas conexões, entende-se que um perfil em um site de rede social fornece a pessoas mal intencionadas subsídios suficientes para ataques de engenharia social. O álbum de fotos, por exemplo, indica o ciclo de amizades, locais que o usuário frequenta e seus hábitos pessoais, principalmente pela opção de marcar pessoas e lugares. A lista de grupos identifica os grupos sociais da qual o usuário faz parte. Já os comentários e a agenda de eventos podem oferecer informações como os amigos mais íntimos, encontros, planos e compromissos futuros do usuário. Além dessas ameaças, os aplicativos, como o *Instagram* e o *Fousquare*, disponibilizam informações quase instantâneas sobre o lugar em que o usuário se encontra, seja através da identificação dos lugares na foto, seja pela localização no mapa associado ao aplicativo.

A partir do levantamento dessas vulnerabilidades, o CERT (2012) divulgou uma Cartilha de Segurança para Internet, a fim de orientar os usuários no gerenciamento das informações que são disponibilizadas na rede e, mais especificamente, nas redes sociais. Os principais riscos apontados na Cartilha são: furto de identidade (perfil falso); invasão de perfil (através do uso de páginas falsas ou computadores infectados); uso indevido de informações (incluindo o uso de questões de segurança usadas para recuperação de senhas); vazamento de informações (conteúdos sigilosos de empresas divulgados na Internet); disponibilização de informações confidenciais (persuasão para fornecimento de e-mail, endereço, telefone, etc); sequestro (através da localização do usuário por meio do uso de aplicativos para fazer *check-in* em lugares como restaurantes, cinemas e outros); furto de bens (comentários de que estará fora de casa num determinado período); recebimento de mensagens maliciosas; acesso a conteúdos impróprios ou ofensivos; danos à imagem e à reputação (ex.: calúnia e difamação).

Com a finalidade de prevenir esses ataques, o Facebook disponibiliza algumas configurações de segurança e privacidade para os seus usuários. Uma das principais é a possibilidade de classificação da informação (postagens, fotos e vídeos) nas opções: público, para amigos, somente para o próprio usuário, personalizado (pessoas) ou por lista (grupo de pessoas). Outras opções disponíveis são: a ativação da navegação segura; notificação de *login* quando a conta for acessada de um computador ou dispositivo móvel não cadastrado; ativação de um código de segurança para acessar a conta a partir de navegadores desconhecidos; utilização de senha específica para uso de aplicativos (em vez de utilizar a mesma senha do Facebook).

Dentre as outras opções de segurança e privacidade, o Facebook disponibiliza ainda ao usuário, na sua Central de Ajuda, informações sobre: Como fazer para bloquear alguém? Como controlar quem pode o localizar no Facebook com suas informações de contato? Como

controlar quem pode lhe enviar mensagens? Como fazer para controlar quem pode ver publicações e fotos nas quais está marcado em sua linha do tempo? Como ativar a opção para analisar marcações que amigos adicionam às publicações antes de elas aparecerem? Como denunciar problemas (com base nos padrões da comunidade do Facebook)? Além dessas, são fornecidas informações sobre o gerenciamento de aplicativos e de conexões. Todas essas informações estão coerentes com as sugestões necessárias à gestão da segurança da informação publicadas pelo CERT.

Nesse sentido, se torna importante a atenção dos usuários às pessoas adicionadas a sua rede de amizades, é necessário atenção para o uso correto das ferramentas de gerenciamento da informação, observando o tipo de conexão estabelecida com os outros usuários, tais como amigos, melhores amigos, conhecidos, e integrantes de listas/grupos específicos.

As pessoas são consideradas um elo frágil nos sistemas de segurança da informação, seja ele físico ou virtual, sendo necessário a valorização de políticas de segurança da informação e treinamentos nos ambientes intraorganizacional e doméstico para sensibilização e conscientização das vulnerabilidades e ameaças existentes por meio da atuação da engenharia social e sua maximização por meio do uso de redes sociais na Internet, como também se faz necessária a realização de treinamentos sobre o uso correto dos sites de redes sociais e suas configurações de segurança e privacidade.

3 POLÍTICAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Nos ambientes corporativos, para sanar ou minimizar os diferentes tipos de falha humana é necessária a criação de diretrizes organizacionais que estabeleçam normas de conduta – as Políticas de Informação. De acordo com Basto (2012), uma política de segurança da informação pode ser definida como "um documento que registra os princípios e as diretrizes de segurança adotado pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos." É por meio delas que as empresas planejam sua defesa diante de um possível ataque de um engenheiro social, entre outras ameaças.

Para isso, se faz necessário um trabalho contínuo, planejado, coordenado e executado com acompanhamento de profissionais capacitados para esse objetivo. A partir do planejamento, as seguintes etapas são cumpridas para a execução de uma Política de Informação: (1) Avaliação de riscos – Identificação e análise das vulnerabilidades existentes no ambiente; (2) Análise do custo/benefício da informação – verificação dos tipos de informação que devem ser protegidos na organização; (3) Criação de diretrizes e sua formalização em políticas (normas e procedimentos) e sua divulgação; (4) Pesquisa contínua para atualização da política –

verificando se as diretrizes determinadas e implementadas estão proporcionando resultados eficientes; (5) Programa de treinamento e conscientização dos usuários – primordial para a execução das diretrizes estabelecidas; e (6) Plano de gestão de crise (incidentes) – plano de contínua atualização e devido monitoramento.

Sendo assim, a conscientização dos usuários e a execução de uma política de gestão de segurança da informação tornam-se essenciais para as empresas, assim como estratégias adequadas devem ser pensadas pelo indivíduo comum no uso de redes sociais *online,* a fim de evitar ataques de engenheiros sociais e suas consequências morais ou financeiras. Para exemplificar a importância deste conteúdo será apresentado a seguir um estudo de caso demonstrando como alguns indivíduos estão expostos nas redes sociais *online.*

4 PROBLEMATIZAÇÃO, OBJETIVO E JUSTIFICATIVA

Com o aumento da exposição de informações pessoais na Web, é natural que aumente também os riscos associados a estas. Mas como mensurar quanto as informações de determinado indivíduo estão expostas? Para responder tal questão, este trabalho teve como **objetivo analisar o grau de exposição de informações de pessoas físicas acessíveis na Web.**

Até maio de 2013, em consulta realizada à Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI), não foi encontrada nenhuma publicação na área de Ciência da Informação que aborde este tema no Brasil. É nesse aspecto que se justifica uma pesquisa que demonstre como estas informações postadas na Web estão expostas às técnicas de engenharia social, por meio da aplicação de uma métrica para se mensurar o grau de exposição dos indivíduos, cujos resultados podem auxiliar em programas de conscientização e servir de alerta para os usuários da rede. A facilidade de acesso e o uso indevido de informações pessoais fizeram com que o *The Federal Bureau of Investigation- FBI* promovesse em 2012 uma campanha de alerta nos EUA. Segundo o FBI:

> Uma vez que a informação é publicada em uma rede social, esta já não é privada. Quanto mais informações um indivíduo publica, mais vulnerável se torna. Mesmo quando se utiliza configurações de segurança elevadas, amigos ou sites podem, inadvertidamente, vazar as informações. (UNITED STATES, 2012, tradução nossa)

Para fins deste trabalho utiliza-se como base a definição de "informação pessoal" apresentada no Decreto nº 7.724, de 16 de maio de 2012 – "informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem" (BRASIL, 2012).

5 DESENVOLVIMENTO, ANÁLISE E DISCUSSÕES

Diante do grande volume de informações pessoais disponíveis na Internet e na perspectiva de entender na prática as vulnerabilidades e ameaças existentes nesse ambiente, a presente pesquisa se propôs a fazer um levantamento das informações pessoais sobre determinados usuários que estão disponíveis na rede e promover uma discussão sobre o seu potencial de uso em ataques de engenharia social. Para tanto, a pesquisa foi desenvolvida como um estudo de caso. É caracterizada como de abordagem quantitativa e qualitativa, focando no levantamento de informações pessoais e profissionais, utilizando-se de consultas a sites e portais de acesso livre na Web, ferramentas de busca, e na análise de conteúdos e imagens em perfis de usuários cadastrados no site de rede social Facebook. Este SRS foi selecionado devido à grande visibilidade dos usuários e aos tipos de ameaças já mencionadas na revisão de literatura relacionada ao seu uso.

Para a realização deste trabalho foi utilizada uma amostragem do tipo não probabilística. A amostra foi composta por integrantes de uma turma do curso de mestrado em Ciência da Informação do PPGCI/UFPB, totalizando 10 (dez) pessoas. Ressalta-se, no entanto, que nenhum dos perfis analisados estava na "lista de amigos" no Facebook dos pesquisadores no momento da análise. A coleta de dados aconteceu entre janeiro e março de 2013. Conforme verificado na fundamentação teórica, foram trabalhadas as seguintes variáveis relacionadas com "informações pessoais": número de RG; número de CPF; gostos/preferências; data de aniversário; informações sobre família; lugares que frequenta/frequentou; status de relacionamento (companheiro (a)); endereço residencial; e-mail pessoal e/ou profissional; telefone/celular pessoal e/ou profissional; profissão; local de trabalho; rendimentos; e educação.

A primeira parte da pesquisa, apresentada na Figura 1, se limitou ao levantamento de número de RG e CPF no Google, utilizando-se do nome completo dos integrantes da amostra e as variáveis como palavras-chave na busca pelos termos.

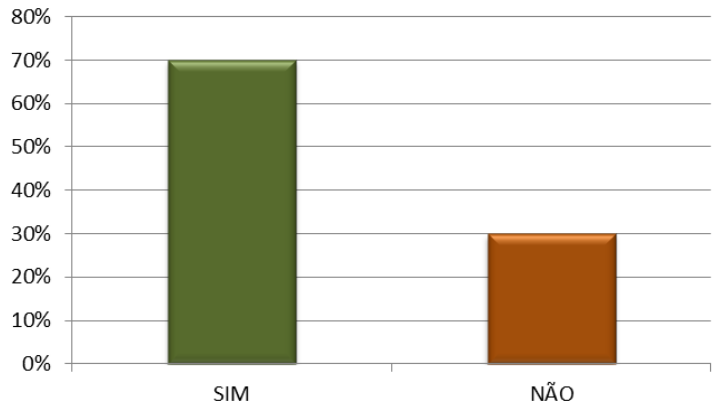

Figura 1 – Dados de RG e CPF identificados.
Fonte: Elaborado pelos autores (2013)

Do total de membros pesquisados, 70% possuem o número de RG e 30% possuem o número de CPF disponíveis na Internet. Conforme os documentos visualizados, esses dados podem ser identificados quando o indivíduo participou de algum tipo de concurso, prova de vestibular etc. já que a lista de classificados/aprovados normalmente é divulgada com a identificação numérica do participante, seja o RG ou CPF.

Verificou-se que do total de membros pesquisados, 70% possuem perfil ativo no Facebook. Uma vez identificado um perfil no Facebook, torna-se fácil encontrar informações relacionadas às outras variáveis já mencionadas e que podem ser visualizadas na Figura 2. Em 50% do total da amostra foi possível identificar as preferências quanto a times de futebol, esportes, músicas, leituras etc. Em 40%, a data de aniversário está disponível na opção "público", ou seja, qualquer usuário do Facebook, mesmo que não esteja incluído na sua lista de amigos, pode visualizar essa informação.

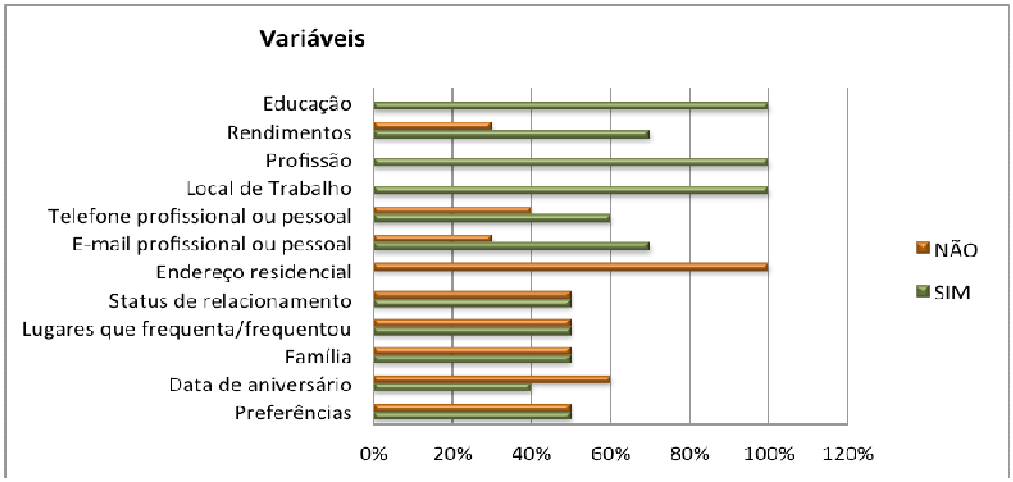

Figura 2 – Informações pessoais identificadas na Internet.
Fonte: Elaborado pelos autores (2013)

Em relação à **marcação de familiares**, 50% dos pesquisados marcam pais, filhos, irmãos e primos na opção "público". Já em relação aos **lugares que frequenta/frequentou**, não foi possível verificar em 50% dos usuários analisados, pois estes não utilizam muitas marcações em fotos, como também não utilizam ferramentas de geolocalização, como por exemplo, o *Fourquare*, pelo menos não com a opção "público". As informações identificadas foram complementadas com a análise de comentários postados em fotos e publicações na *timeline* do usuário. Já em relação ao **status de relacionamento**, 50% dos usuários pesquisados apresentam essa informação na opção "público" com a identificação da(o) respectiva(o) parceira(o). Vale destacar que só foi possível encontrar essas informações nos usuários que possuem perfil no Facebook.

Em relação ao **endereço residencial**, 100% dos pesquisados não possuem essa informação disponível na Internet, como também não a possuem no Facebook em formato público. Já o **e-mail e o telefone** (profissional ou pessoal) são encontrados em 70% e 60% deles, respectivamente, porém nenhum contato é visualizado pelo Facebook, mas sim por meio de buscas pelo Google. Já em relação à **educação** e ao **local de trabalho**, 100% dessas informações são visíveis para o público. Outra informação possível de ser levantada na Internet é o salário-base dos integrantes da amostra identificados como servidores públicos federais ou bolsistas de graduação ou de pós-graduação. No caso desta pesquisa, 60% eram servidores públicos e 10% bolsistas, cujas informações de salários ou bolsas estão disponíveis no Portal de Transparência Pública do Governo Federal[1] ou em sites de órgãos públicos, como também no portal da CAPES[2] ou no CNPq.[3]

Para um Engenheiro Social, esse tipo de exposição de informações facilita tanto a aproximação com o usuário quanto o uso indevido destas informações para a construção de perfis falsos, chantagens, sequestros, ou até mesmo a manipulação e influência para a transmissão de informações sigilosas e importantes, seja para a pessoa ou para a organização (HADNAGY, 2011, p. 31).

Saber onde localizar o indivíduo, conhecer sua rotina, gostos e preferências, familiares, companheiros (as), entre outras informações consideradas críticas, favorece o enriquecimento de sua argumentação e estratégias para cometer qualquer tipo de ato criminal, pois há uma superexposição da qual os indivíduos ainda não se deram conta, cada vez mais fazendo uso dos recursos disponíveis para se expor em público. Tal fenômeno é conhecido como “hipermobilidade estética dos internautas” (STASSUN; ASSMANN, 2012).

Como não foi identificado na literatura (ALVES, 2010; BRAGA, 2011; CAVALCANTI JUNIOR, 2011; LENNERT; OLIVEIRA, 2011; PEIXOTO, 2006) um modelo para mensurar o grau de exposição de cada individuo, foi necessário elaborar um método com uma escala de classificação. Este foi desenvolvido com base no *Facilitated Risk Analysis and Assessment Process* (FRAAP) utilizado para análise de risco em segurança da informação. Segundo Peltier (2005, p. 129), o FRAAP é um processo testado, eficiente e organizado para assegurar que os riscos relacionados à segurança das operações dos negócios sejam detectados e documentados.

Na presente pesquisa, foi atribuído um peso para cada variável relacionada à informação pessoal, considerando a possibilidade de se usar tal informação em uma fraude, como por exemplo, para criação de um cadastro falso. As variáveis pesquisadas foram

[1] http://www.portaltransparencia.gov.br/
[2] http://www.capes.gov.br/bolsas/bolsas-no-pais
[3] http://www.cnpq.br/no-pais

classificadas, e a cada categoria atribuiu-se uma pontuação conforme sua criticidade, resultando na seguinte disposição:

1. informações sobre rendimentos (4 pontos): variável - rendimentos.

2. informações usadas em cadastros (3 pontos): variáveis - número de rg; número de cpf; data de aniversário.
3. informações que permitem localizar e/ou entrar em contato direto com o usuário (2 pontos): variáveis - endereço residencial; e-mail pessoal e/ou profissional; telefone/celular pessoal e/ou profissional; local de trabalho.
4. demais informações (1 ponto): variáveis - informações sobre família; lugares que frequenta/frequentou; status de relacionamento (companheiro (a)); gostos/preferências; profissão e educação.

Para tabulação da exposição a que os usuários estão sujeitos foi proposta a seguinte escala:

- zero – sem exposição;
- de um até 10 pontos – exposição baixa;
- de 11 até 20 pontos – exposição alta;
- de 21 até 27 pontos – exposição extrema.

Os resultados do FRAAP são apresentados em um conjunto de documentos (tabelas) que identificam as ameaças e permite priorizá-las em níveis de risco, além de identificar possíveis controles que ajudarão a reduzir esses riscos. Para implementação desta pesquisa foi desenvolvido procedimento similar, no qual, identificado uma das variáveis, a pontuação foi distribuída para cada indivíduo estudado, conforme demonstrado na tabela 1.

Tabela 1 – Pontuação para variáveis identificadas na Web.

Variáveis/indivíduos	i-1	i-2	i-3	i-4	i-5	i-6	i-7	i-8	i-9	i-10
data de aniversário	0	0	3	0	0	0	3	3	3	0
educação	1	1	1	1	1	1	1	1	1	1
e-mail pessoal e/ou profissional	2	0	2	2	0	2	2	2	0	2
endereço residencial	0	0	0	0	0	0	0	0	0	0
gostos/preferências	0	1	1	0	0	1	0	1	1	0
informações sobre família	0	0	1	0	0	1	1	1	1	0
local de trabalho	2	2	2	2	2	2	2	2	2	2
lugares que frequenta/frequentou	0	1	1	0	0	1	0	1	1	0
número de CPF	0	0	3	3	3	0	3	3	3	3
número de RG	3	3	3	3	3	0	0	0	3	3
profissão	1	1	1	1	1	1	1	1	1	1
rendimentos	4	4	4	0	0	4	4	4	0	4
status de relacionamento (companheiro (a))	1	0	1	0	0	1	0	1	1	0
telefone/celular pessoal e/ou profissional	2	0	2	0	0	2	2	2	0	2
Total	**16**	**13**	**25**	**12**	**10**	**16**	**19**	**22**	**17**	**18**

Fonte: Elaborado pelos autores (2013)

Os resultados podem ser visualizados na Figura 3. Ressalta-se que a métrica elaborada e aplicada nesta pesquisa não indica o nível do risco, mas somente o grau de exposição do usuário. Para identificar o risco, é necessário complementar o estudo com uma análise de riscos. Da amostra estudada, 70% apresentam um indicador alto e 20% extremamente alto de exposição das informações pessoais na Web. Nenhum dos indivíduos pesquisados apresentou grau zero de exposição, o que era previsível, pois se tratava de alunos de pós-graduação. Este tipo de usuário apresenta um elevado grau de uso da internet e de redes sociais.

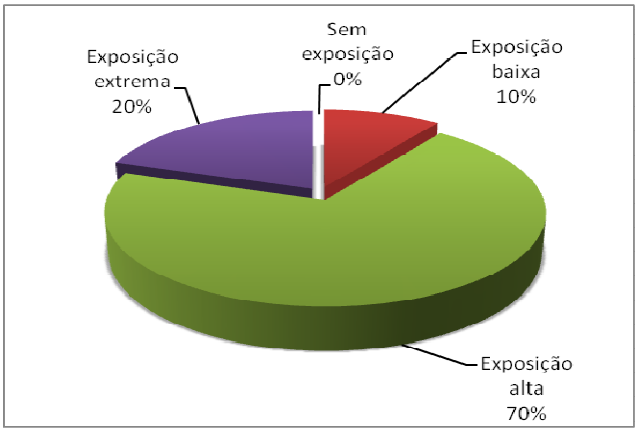

Figura 3 – Grau de exposição dos usuários
Fonte: Elaborado pelos autores (2013)

Como a amostra foi composta por um número reduzido de pessoas, não é possível fazer generalizações, mas os resultados obtidos permitem criar hipóteses que podem ser trabalhadas em uma pesquisa com uma amostra probabilística que represente uma parcela mais significativa de uma determinada população.

A partir desse levantamento de informações dos membros do PPGCI/UFPB na Internet, foi possível demonstrar a facilidade na busca e encontro de informações referentes a um determinado usuário no ambiente online. Com as diferentes ferramentas e pesquisas não é difícil unir informações sobre uma pessoa, suficientes para ataques de engenharia social. Nesse contexto é de fundamental importância a abordagem da segurança da informação na Internet, mais especificamente, nas redes sociais, para o uso correto do ambiente virtual de forma que os usuários não aumentem as ameaças existentes nesse ambiente, seja por falta de conhecimento sobre configurações de segurança e privacidade, seja devido às características de comportamento pessoal que tornam o ser humano vulnerável à quebra de segurança pela comunicação interpessoal e pelo relacionamento virtuais.

Considerando que a existência dessas ameaças estão relacionadas direto com as pessoas, e estas fazem podem atuar ou trabalhar em diferentes tipos de organizações, sua participação displicente nas redes sociais pode trazer prejuízos as organizações quanto ao uso das informações de forma intencional ou involuntária.

Ressalta-se portanto, a necessidade de implantação de políticas de gestão da segurança da informação no ambiente organizacional, contribuindo para a capacitação dos usuários quanto ao uso correto do ambiente virtual e conscientização dos indivíduos quanto às técnicas existentes de engenharia social.

6 CONSIDERAÇÕES FINAIS

Com base na fundamentação teórica e nos resultados obtidos pelo estudo de caso apresentado, observa-se a facilidade de encontrar informações pessoais na Internet por meio de mecanismos de busca que não são necessariamente sofisticados, ou que não necessitam de conhecimento avançado para seu uso. Por meio da busca de número de CPF e RG, por exemplo, percebe-se que as pessoas que prestaram algum concurso público possuem essas informações disponibilizadas pelos editais de homologação ou de classificação, ou ainda de aprovação.

As informações sobre bolsas de estudo e remuneração são encontradas facilmente no site da CAPES/CNPq, no Portal de Transparência Pública do Governo Federal, ou até mesmo de outros órgãos, como os Tribunais Regionais do Trabalho, os Tribunais de Contas do Estado, ou pelo Tribunal de Contas da União.

Contudo tais informações deveriam ser protegidas, conforme Lei 12.527/2011 em seu capítulo II, que trata "do acesso a informações e da sua divulgação" no Art. 6º determina que "cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso."

Contudo, em alguns casos, a interpretação desta acontece de forma equivocada, conforme alertado por Araújo (2012), a mesma deveria garantir a proteção do sigilo das informações pessoais, que é definida como "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011), contudo o Portal da Transparência disponibiliza a informação sobre remuneração de grande parte dos funcionários públicos federais, sem antes refletir se esta é uma informação pessoal ou não, tornando tais indivíduos mais vulneráveis. Tal

informação, assim como as muitas outras que podem ser encontradas por meio dos sites de relacionamento (Ex.: *Facebook)* podem ser utilizadas (de forma complementar) por engenheiros sociais para uso indevido em ataques – golpes financeiros ou morais (de imagem), sejam eles contra pessoas ou organizações. Portanto, fica evidente a importância de uma abordagem estratégica para o gerenciamento da segurança da informação.

Nos ambientes organizacionais, faz-se necessária a implantação de políticas de segurança da informação, que atentem tanto para a capacitação dos usuários, configuração e uso corretos de ferramentas e para a preservação da privacidade, quanto para a conscientização acerca das vulnerabilidades e ameaças existentes no relacionamento interpessoal e na comunicação humana, principalmente no ambiente virtual, bem como acerca dos comportamentos de prevenção a tais ataques de engenharia social.

7 Referências

ALVES, Cássio Bastos. **Segurança da informação vs. engenharia social**: como se proteger para não ser mais uma vítima. 2010. 63f. Monografia (Graduação em Sistemas de Informação) – Coordenação do Curso de Sistemas da Informação, Centro Universitário do Distrito Federal, Brasília, 2010.

ARAÚJO; Wagner Junqueira de. Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. **Informação & Sociedade**: Estudos, João Pessoa, v. 22, número especial, p. 13-24, 2012. Disponível em: <http://www.ies.ufpb.br/ojs/index.php/ies/article/view/13675/8206>. Acesso em: 22 maio 2013.

BASTO, Fabrício. **Política de segurança da informação**: como fazer?. 2012. Disponível em: <http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/>. Acesso em 05 dez. 2012.

BOYD, D. M.; ELLISON, N. B. Social network sites: definition, history, and scholarship. **Journal of Computer-Mediated Communication**, v. 13, n. 1, 2007. Disponível em: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>. Acesso em: 05 dez. 2012.

BRAGA, Pedro Henrique da Costa. **Técnicas de engenharia social**. 2010. Disponível em <http://pt.scribd.com/doc/133664659/Tecnicas-de-Engenharia-Social >. Acesso em: 14 out. 2012.

BRASIL. Presidência da República. **Decreto Nº 7.724, de 16 de maio de 2012**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do §3 do art. 37 e no §2 do art. 216 da Constituição. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm>. Acesso em: 22 mai. 2013.

BRASIL. Lei 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 de Nov. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 08 de ago. 2012.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 3. ed. Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059160.PDF>. Acesso em: 14 dez. 2012.

CAVALCANTI JUNIOR, Reinaldo Leopoldino. **Engenharia social nas redes sociais.** 2011. 48 f. Monografia (Especialização em Desenvolvimento de Sistemas para Web) – Departamento de Informática, Universidade Estadual de Maringá, Maringá, 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet**. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 14 dez. 2012.

FURLAN, Paula. **10 estatísticas curiosas sobre o Facebook no mundo**. 2012. Disponível em: <http://consumidormoderno.uol.com.br/empresas/10-estatisticas-curiosas-sobre-o-Facebook-no-mundo>. Acesso em 14 dez. 2012.

DAMASCENO, Sérgio. **Brasil é o 10º país em adesão a redes sociais**. 2012. Disponível em: <http://www.meioemensagem.com.br/home/midia/noticias/2012/02/29/Brasil-e-o-1o--pais-em-adesao-a-redes-sociais.html#ixzz2FHnrCkH3>. Acesso em 15 dez. 2012.

FACEBOOK. Disponível em: <https://www.facebook.com/>. Acesso em: 14 dez. 2012.

FERNÁNDEZ, J. R. Coz et al. Evaluación de la privacidad de una red social virtual. **Ibérica de Sistemas e Tecnologias de Informação**, Madri, n. 9, 2012.

HADNAGY, Christopher**. Social engineering:** the art of human hacking. Indianapolis: Wiley Publishing, 2011.

G1. **Crime cibernético gera prejuízos de quase R$ 16 bilhões só no Brasil**. 2012. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/10/crime-cibernetico-gera-prejuizos-de-quase-r-16-bilhoes-no-brasil.html>. Acesso em: 14 dez. 2012.

HISTÓRIA dos sites de relacionamentos e seus riscos. [20--]. Disponível em: <https://sites.google.com/site/historiasobreossitesdebusca/historia-dos-sites-de-relacionamento/historia-dos-sites-de-relacionamento-e-seus-riscos>. Acesso em: 14 dez. 2012.

JÚNIOR, Guilherme. **Entendendo o que é engenharia social**. 2006. Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 05 dez. 2012.

LENNERT, Luiz Sérgio; OLIVEIRA, Marcos Altermari. O que é engenharia social? **Gestão de Riscos**, São Paulo, ed. 64, mar. 2011. Disponível em: <http://www.brasiliano.com.br/revista.php>. Acesso em: 05 dez. 2012.

MITNICK, Kevin D.; SIMON, William L. Mitnick: **A arte de enganar.** São Paulo: Pearson Makron Books, 1963.

PEIXOTO, Mário C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PELTIER, Thomas R. **Information security risk analysis.** 2nd ed. United States: CRC Press; Taylor & Francis Group, 2005.

PROMON BUSINESS & TECHNOLOGY REVIEW. **Segurança da informação**: um diferencial determinante na competitividade das corporações. 2005. Disponível em: <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf>. Acesso em: 05 dez. 2012.

RECUERO, Raquel. **Redes sociais na internet.** Porto Alegre: Sulina, 2009.

SAFERNET Brasil. Disponível em: <http://www.safernet.org.br>. Acesso em: 14 dez. 2012.

SÊMOLA, Marcos. Gestão da segurança da informação. In: STAREC, Cláudio; GOMES, Elizabeth; BEZERRA, Jorge (Org.). **Gestão estratégica da informação e inteligência competitiva.** São Paulo: Saraiva, 2006.

SINGH, Simon. **O livro dos códigos:** a ciência do sigilo: do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

SOCIAL Bakers. **Brazil Facebook statistics**. Disponível em: <http://www.socialbakers.com/Facebook-statistics/brazil>. Acesso em: 14 dez. 2012.

STASSUN, Cristian Caê Seemann; ASSMANN, Selvino José. Hipermobilidade estética e dispositivos de controle de circulação: o desejo de ser notado e encontrado na internet. **Cadernos de Pesquisa Interdisciplinar em Ciências Humanas**, Florianópolis, v. 13, n. 102, p. 153-177, jan./jun. 2012. Disponível em: <http://www.periodicos.ufsc.br/index.php/cadernosdepesquisa/article/view/24238>. Acesso em: 10 fev. 2013.

UNITED STATES. Department of Justice. Federal Bureau of Investigation**. Internet social networking risks**. [s. d.]. Disponível em: <http://www.fbi.gov/about-us/investigate/counterintelligence/Internet-social-networking-risks-1>. Acesso em: 22 mai. 2013.