Revista de Sistemas de Informação da FSMA
n. 16 (2015) pp. 71-81

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

Caracterização Qualitativa das Estratégias de Segurança da Informação do Facebook

Silmara Ferreira Lopes[1], Glívia Angélica Rodrigues Barbosa[2], Marcelo Werneck Barbosa[1]
[1]Instituto de Ciências Exatas e Informática – PUC Minas
[2]Departamento de Computação – CEFET Minas
silmara.lopes@sga.pucminas.br, gliviabarbosa@decom.cefetmg.br, mwerneck@pucminas.br

***Abstract*—Hyperconnectivity due to online social networks exposed security issues on data stored in these systems. This article presents an analysis on how online social networks designers have been communicating information security aspects through these systems' interfaces. This analysis was made using the Semiotic Inspection Method on Facebook since it is largely used in Brazil and all over the world. Results showed that there is major concern with security information properties. Nevertheless it was possible to identify interface problems that could compromise use and understanding of such security properties.**

Index terms* - *Semiotic Inspection Method. Social networks. Information Security

***Resumo* - A hiperconectividade proporcionada pelas redes sociais online trouxe questionamentos sobre a segurança dos dados expostos através desses sistemas. Esse artigo apresenta uma análise sobre como os projetistas de redes sociais online têm comunicado aspectos de segurança da informação, por meio de suas interfaces. A referida análise foi realizada utilizando o Método de Inspeção Semiótica no Facebook, uma vez que essa rede social é considerada um fenômeno de utilização no Brasil e no mundo. Os resultados mostraram que existe uma preocupação com as propriedades de segurança da informação, mas foi possível identificar problemas na interface que podem comprometer o entendimento e bom uso dessas propriedades de segurança.**

Palavras-chave - Segurança da Informação, Redes Sociais, Método de Inspeção Semiótica.

I. INTRODUÇÃO

Segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação [6], com o grande avanço da tecnologia, têm-se acesso às informações instantaneamente e junto com essa facilidade, surgem diversas ameaças, ataques e crimes, que podem trazer grandes danos morais, financeiros e até mesmo físicos para as organizações e/ou pessoas. Estes estudos ainda apontam um crescimento contínuo ao longo dos últimos anos do número de incidentes de segurança da informação.

Albesher e Alhussain [1] apresentam estudos que mostram que trabalhos realizados na área de Segurança da Informação estão mais centrados em aspectos tecnológicos e matemáticos e que pouco tem sido produzido sobre aspectos sociais da Segurança da Informação. As organizações dispõem de tecnologias voltadas para esse objetivo e elaboram políticas, normas e procedimentos tecnicamente completos, mas incompletos por não tratarem corretamente das relações humanas envolvidas, o que permite ataques, por exemplo, do tipo Engenharia Social.

As redes sociais são uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns [10]. Já uma rede social *online* é uma plataforma que oferece um espaço de comunicação e de interação digital a conjuntos de pessoas com necessidades e interesses semelhantes [11].

Redes sociais *online* são aplicações baseadas na web que as pessoas usam para se conectar com outras com as quais elas compartilham interesses comuns, tanto profissionais quanto pessoais. Usuários publicam conteúdos na aplicação para atualizar conexões e compartilhar notícias pessoais, interesses, entre outros. Isso pode ser realizado na forma de atualizações de textos simples, vídeos ou fotos.

As pessoas usam redes sociais para encontrar trabalho, novos clientes ou estar em contato com familiares e amigos distantes. Exemplos de redes sociais online são o LinkedIn, Facebook, Twitter e YouTube. Redes sociais *online* geralmente oferecem aplicações adicionais que estendem sua funcionalidade como jogos ou *quizzes* que foram desenvolvimentos por parceiros e têm o potencial de introduzir riscos de segurança [17], tais como quando solicitam dados de sua conta para acesso à funcionalidade. Situações como esta podem gerar invasão de perfil ou vazamento de informações. Com o crescimento das redes sociais *online*, o problema da vulnerabilidade em relação à segurança e privacidade das informações se agrava. A exposição de informações pessoais ainda é potencialmente grande.

É razoável supor que casos como a penetração da rede do PlayStation, ocorrido em 2011, permitem inferir que qualquer aplicativo online que armazene informações online pode ser alvo de ataques. Entretanto, neste trabalho vamos focar apenas nas redes sociais, mas isto não quer dizer que os conceitos deste trabalho não sejam extensíveis a outros tipos de redes.

Empresas de mídias sociais como Facebook, Google e Twitter geralmente têm suas próprias políticas de privacidade que governam o uso de dados dos clientes e conduta de terceiros nas redes com respeito a dados pessoais [4]. Entretanto, as próprias redes sociais não deixam claras quais são suas políticas de privacidade, colocando o usuário em risco, conforme aponta um levantamento realizado pelo Instituto Brasileiro de Defesa do Consumidor [14]. Em análise feita nas redes sociais mais populares do Brasil, entre elas o Facebook [7], constatou-se que, embora a rede não cobre pelos seus serviços, os usuários são obrigados a fornecer seus dados pessoais sem saber o que será feito com eles e acabam aceitando as condições de uso.

De certa forma, isto é similar ao que se faz em uma loja física, o que permite dizer que ambas as situações são arriscadas. Entretanto, no caso de redes sociais, o alcance dessa exposição é potencialmente maior uma vez que a informação é compartilhada com mais agilidade e, ademais, na rede social é mais difícil encontrar a origem de um vazamento de informação, entre outros problemas inerentes à sua arquitetura e concepção.

A segurança e a privacidade relacionadas aos sites de redes sociais são fundamentalmente assuntos comportamentais e não tecnológicos. Quanto mais informação uma pessoa publica, mais informação se torna disponível para uso indevido ou com intenções maliciosas. Publicar fotos, vídeos ou arquivos de áudio pode levar à quebra da privacidade de um indivíduo [17].

O principal responsável pela privacidade e segurança é o próprio usuário. Uma informação postada pode se propagar e, algo que deveria ser uma brincadeira entre amigos, pode ser acessada por outras pessoas e ser usada contra o usuário agora ou futuramente [18]. Contudo, embora essa responsabilidade seja atribuída principalmente ao usuário, a solução tecnológica deve oferecer mecanismos para que o próprio usuário proteja a segurança de suas informações [36][37].

Nos últimos anos, a popularidade de redes sociais *online* tem crescido enormemente [9], [15]. Entretanto, redes sociais atraem não somente usuários de boa fé, mas também usuários de má índole [15]. Assim, proteger a privacidade, compartilhar informações e aplicações em redes sociais *online* ou na Internet são problemas muito importantes. [33].

Esta é uma necessidade tão premente que recentemente o Facebook anunciou novas configurações de privacidade. Apesar de serem grandes avanços, pesquisadores e especialistas continuam criticando tais configurações, pois elas precisam ser melhoradas e simplificadas [33].

Por outro lado, o tema de segurança da informação em redes sociais *online* não tem recebido a devida atenção das pesquisas acadêmicas, como mostra o trabalho de Albuquerque e Santos [2], que realizaram uma análise das publicações brasileiras sobre Segurança da Informação sob a ótica social em periódicos científicos entre 2004 e 2013. A pesquisa mostrou que poucos periódicos consultados publicaram artigos sobre Segurança da Informação com um enfoque social nos últimos 10 anos e que os trabalhos normalmente possuem foco na importância das normas e padrões de Segurança da Informação.

Dado este contexto, existem dúvidas sobre como os dados fornecidos pelo usuário serão manipulados. Este trabalho parte da premissa que tais dúvidas podem estar relacionadas a problemas de interface, uma vez que o projetista da interface e da interação pode não comunicar bem sua intenção aos usuários. Assim, as pessoas que utilizam o Facebook necessitam de alguns conhecimentos prévios e de algum tipo de experiência com interfaces de sistemas computacionais e sistemas web para uma boa utilização do software.

Assim, este trabalho consiste em analisar como o projetista comunica através da interface do sistema, as propriedades da segurança da informação dentro do contexto da rede social do Facebook. Para isto, foi utilizado o Método da Inspeção Semiótica de caráter qualitativo [22], e a partir dos resultados obtidos, foi apresentada a maneira como a comunicação das propriedades é feita para o usuário, bem como as estratégias adotadas pelo projetista nessa comunicação e os potenciais problemas de segurança que poderiam ser vivenciados pelos usuários, em tempo de interação.

Os resultados dessa análise e caracterização poderão orientar a melhoria e/ou o desenvolvimento de soluções que potencializem a segurança da informação em redes sociais, uma vez que identificam as estratégias usadas pelo Facebook e problemas identificados na interface relativos à apresentação de questões de segurança.

O restante deste trabalho está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve os procedimentos metodológicos adotados assim como o referencial teórico. A Seção 4 apresenta a apreciação da proposta de segurança da informação do Facebook bem como rupturas de segurança identificadas neste trabalho enquanto a Seção 5 descreve as conclusões e trabalhos futuros.

II. TRABALHOS RELACIONADOS

Há modos de se proteger a privacidade, controlar a segurança, status de relacionamento, outras informações e categorizar as listas de amigos para limitar acesso indevido. O estudo realizado por Yuksel, Yuksel e Zaim [33] provê uma implementação de uma solução web para proteção da privacidade da informação. Esta solução auxilia os usuários a automaticamente categorizar um grande número de amigos em listas de classificação. A principal premissa desse trabalho é que usuários tendem a apresentar as mesmas informações para todos os amigos em um grupo social e assim círculos sociais proveem uma maneira de se categorizar os amigos e estabelecer políticas de segurança e privacidade. A abordagem é baseada na construção de um grafo visual de grupos sociais e no estabelecimento de políticas para proteção de informação pessoal. Esta abordagem sugere o conjunto de listas de amigos que devem ser criadas e como os amigos atuais devem ser distribuídos a estas listas.

O trabalho de Ngeno et al. [19] realizou uma replicação de uma pesquisa em pequena escala que focou em usuários com alto grau de conhecimento e interesse em TI e na expressão de suas necessidades e requisitos. Usando uma série de entrevistas, alguns usuários foram convidados a relatar suas experiências com sites de redes sociais. Com base nas respostas dadas, percebeu-se que os respondentes desejam mais transparências, confiança e privacidade no Facebook. Os autores da pesquisa concluíram ainda que os respondentes são conscientes e de certa forma aceitam os problemas de segurança do Facebook.

O trabalho feito por [38] analisou como estudantes de Farmácia realizaram sua configuração de privacidade antes e depois de tomar conhecimento das políticas de segurança do Facebook. O trabalho mostrou que, após conhecer a política, os estudantes optaram por configurações mais seguras e que a divulgação da política teve um impacto positivo no comportamento destes alunos.

A pesquisa feita por Dhami et al. [9] teve como objetivo compreender o impacto de preocupações com segurança, confiança e privacidade ao se compartilhar informações em sites de redes sociais. Usando um questionário *online*, dados empíricos foram coletados de 250 usuários do Facebook de diferentes idades durante um período de 4 meses. Os achados desta pesquisa sugerem que um fator que afetou a confiança no Facebook foram as características de segurança providas por Facebook e uma crença individual que acessar o Facebook pela Internet é seguro. Percebeu-se ainda que a uma forte correlação entre privacidade percebida e confiança percebida pelos usuários.

O trabalho de Albesher e Alhussain [1] teve como objetivo melhorar a proteção de informações pessoais e sensíveis de usuários de sites de redes sociais. Em particular, o trabalho discutiu configurações de privacidade, questões de segurança e aplicações de terceiros envolvendo o Facebook. Os resultados do artigo destacam a necessidade de revisões regulares das configurações de privacidade.

O trabalho de Binden et al. [4] destaca a importância de se configurar de maneira apropriada as configurações de privacidade. Como mais e mais usuários estão prestando menos atenção às configurações de privacidade, recomenda-se mudar as configurações padrão das redes sociais para o mais seguro possível para evitar o vazamento de informações pessoais.

Há ainda alguns artigos que discutem tipos de ataques em redes sociais como os de Hasib [13], Malagi, Angadi e Gull [17] e ainda de Zilpelwar, Bedi e Wadhai [34]. A maioria dos trabalhos nesta área apresentam ataques a redes sociais online e mostram que a privacidade das informações dos usuários é uma grande preocupação nestas redes, mesmo que, em geral, estes trabalhos não apresentem soluções úteis para proteção da privacidade das informações [33]. Além disso, nenhum deles procurou avaliar também como o projetista destas redes transmite as informações relativas a segurança a seus usuários.

III. METODOLOGIA E REFERENCIAL TEÓRICO

Considerando o objetivo desse trabalho, procuramos investigar a seguinte questão de pesquisa: "*Como o projetista comunica através da interface do sistema as propriedades da segurança da informação da rede social do Facebook*?".

A metodologia adotada para responder essa questão consistiu em uma abordagem qualitativa, dividida em duas etapas. A primeira procurou investigar quais são as opções de segurança comunicadas na interface do Facebook. A segunda etapa, por sua vez, procurou investigar qual a relação das possibilidades oferecidas pelo projetista dessa rede social com os pilares de segurança da informação descritos na Seção III B. Para realizar as análises citadas foi utilizado o Método de Inspeção Semiótica (MIS) [22], que será descrito na próxima seção.

A. Método de Inspeção Semiótica

O Método de Inspeção Semiótica (MIS) é um fundamentado na Teoria da Engenharia Semiótica. A Engenharia Semiótica (EngSem) [31] é uma teoria explicativa de Interação Humano Computador (IHC), ou seja, uma teoria que nos permite entender os fenômenos envolvidos no design, uso e avaliação de um sistema interativo [22]. A EngSem oferece explicações para os fenômenos que ocorrem no design, uso e avaliação de um sistema interativo e foca no processo de comunicação entre o designer e o usuário por meio da interface do sistema.

Na EngSem, a interface de um sistema é vista como um caso de metacomunicação (i.e., a comunicação entre o projetista e o usuário), onde é comunicado ao usuário através dessa interface a visão do projetista em relação a quem se destina essa interface, quais problemas ela pode resolver e como interagir com ela. A mensagem que o designer transmite ao usuário é conhecida como metamensagem, que é compreendida pelo usuário à medida que vai interagindo com a interface. Segundo Souza [31] a interface de um sistema é uma mensagem do designer para o usuário cujo conteúdo é:

"*Esta é a minha interpretação sobre quem você é o que eu entendi que você quer ou precisa fazer, de que formas prefere fazê-lo e por quê. Eis, portanto, o sistema que consequentemente concebi para você, o qual você pode ou deve usar assim, a fim de realizar uma série de objetivos associados com esta (minha) visão*".

A metamensagem que o designer emite ao usuário é composta por signos. Um signo é tudo aquilo que significa algo para alguém [21]. A EngSem identifica três tipos de signos: os metalinguísticos, os estáticos e os dinâmicos. Os signos metalinguísticos são aqueles que se referem a outros signos da interface e são usados pelos designers para comunicar aos usuários os significados codificados no sistema e a forma de utilizá-los (e.g., documentação e sistema de ajuda do sistema). Os signos estáticos são aqueles que expressam o estado do sistema. Eles podem ser interpretados apenas olhando-se para a interface (e.g., botões que permitam o fechamento ou minimização de uma janela, ícone de uma pasta na área de trabalho e desenho de uma lupa no campo

pesquisar em um browser). Já os signos dinâmicos expressam o comportamento do sistema e só podem ser percebidos à medida que o usuário interage com o sistema. (e.g., botão excluir torna-se habilitado quando seleciono um e-mail no outlook).

O MIS é um método fundamentado na EngSem [31] para avaliação de sistemas interativos. O MIS analisa a interface do ponto de vista da emissão da mensagem de metacomunicação do designer. O objetivo do MIS é identificar se existem rupturas (i.e, problemas) de comunicação e permitir que o(s) avaliador(es) reconstruam a metamensagem do designer. Esta mensagem é composta por signos que são os elementos da interface.

Para avaliar uma interface o MIS propõe 5 etapas que devem ser seguidas pelo avaliador: (1) inspeção dos signos metalinguísticos; (2) inspeção dos signos estáticos; (3) inspeção dos signos dinâmicos; (4) contraste e comparação entre as mensagens identificadas em cada uma das inspeções e (5) apreciação da qualidade da metacomunicação.

A inspeção do signo metalinguístico consiste em um passo previsto pelo MIS, método utilizado na metodologia. Essa inspeção é feita por especialistas a fim de verificar se de fato as informações explicitas sobre o sistema, que não se restringem à ajuda, estão claras o suficiente para o entendimento do usuário. De acordo com os proponentes do método, esta fase é extremamente importante porque embora na prática alguns usuários não recorram a estas instruções num primeiro momento, elas poderão ser úteis durante dúvidas que ocorram em tempo de interação.

Durante as três primeiras etapas o avaliador deve reconstruir a metamensagem do designer e é sugerido o uso da paráfrase citada no início deste tópico como template. Na quarta etapa é feita uma comparação entre as mensagens de metacomunicação geradas pelo avaliador nos passos anteriores. E finalmente na última etapa se faz uma avaliação da comunicabilidade do sistema inspecionado.

O MIS foi adotado para a avaliação proposta neste trabalho porque, embora originalmente o método tenha sido proposto para avaliar a comunicabilidade dos sistemas, uma revisão na literatura realizada por Reis e Prates [25] revelou que este método também permite identificar as estratégias de *design* comunicadas na interface que de um sistema que visam potencializar determinadas qualidades de uso e/ou propriedades (e.g., sociabilidade e privacidade) [24][3].

Nesse sentido, o trabalho realizado por Coutinho, Prates e Chaimowicz [8], identifica estratégias sonoras para orientação em jogos, através da aplicação do MIS. Já o trabalho realizado por Barbosa, Santos e Pereira [3], utilizou o MIS para identificar estratégias de sociabilidade em redes sociais. Os autores Silva e Oliveira [30] utilizaram o MIS para identificar estratégias de marketing em sites de hotel, e, por fim, o trabalho realizado por Silva e Barbosa [29], adota esse método caracterizar estratégias de gamificação em aplicativos móveis educacionais.

Estes trabalhos justificam a escolha do MIS porque mostram a aplicação do método em contextos similares, permitindo a extrapolação para o caso em estudo.

Todas essas evidências justificam a utilização do MIS na identificação de estratégicas de segurança comunicadas na interface do Facebook. A partir dessa análise, as decisões do projetista dessa rede social foram contrastadas com as estratégias de segurança da informação disponíveis na literatura, de forma a verificar se o Facebook contempla os requisitos mínimos para manter a segurança. Para melhor entender estratégias, a próxima seção descreve conceitos relacionados à segurança da informação bem como propriedades que a sustentam.

B. Segurança da Informação e Estratégias de Segurança

A segurança da informação pode ser compreendida como um agrupamento de práticas e medidas, todas voltadas para a devida proteção de informações e dados, tendo como meta a preservação de sua integridade, confidencialidade, disponibilidade [16]. Segurança da Informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou à indisponibilidade da informação. O conjunto destes três problemas forma o que estamos chamando de segurança e será analisado pelo método MIS.

Pode-se definir Segurança como uma prática adotada para tornar um ambiente seguro (atividade, ação, preservação dos princípios), de caráter interdisciplinar, composta de um conjunto de metodologias e aplicações que visam estabelecer: controles de segurança (por exemplo, de autenticação, autorização e auditoria) dos elementos constituintes de uma rede de comunicação e/ou que manipulem a informação [28].

Toda informação é um ativo, e cada ativo tem o seu valor único para a organização e/ou indivíduo e por isso, precisa ser devidamente protegida contra vários tipos de ameaças para manter a sua integridade, disponibilidade, confidencialidade, autenticidade e legalidade, sendo essas as propriedades da informação [28].

Nesse contexto de proteção e preservação da informação, é necessário entender o significado de um sistema de segurança e quais os pilares e princípios que orientam sua implementação. De acordo com Sêmola [28], a segurança da informação pode ser implantada por um conjunto de cinco propriedades:

- A integridade está relacionada à maneira de se proteger as informações contra qualquer tipo de alterações indevidas, acidentais e/ou propositadas.
- A disponibilidade corresponde ao fato de que a informação esteja acessível no momento em que o indivíduo ou a instituição necessitem dela.
- A confidencialidade está relacionada com a proteção da informação de acordo com o grau de sigilo de seu conteúdo.

- A autenticidade pode ser relacionada a um processo de identificação, uma maneira de garantir que as partes envolvidas são realmente quem afirmam ser.

- E por último, a legalidade está vinculada ao respeito a aspectos legais, como leis, normas e políticas.

Note-se que esses aspectos foram analisados a partir do que estava comunicado na interface. Não partimos deles especificamente, mas sim, analisamos a interface para verificar se eles estavam presentes ou não.

Entre os aspectos observados ainda pela Segurança da Informação está a privacidade dos dados dos usuários, que alguns autores como Sêmola [28], veem como parte da confidencialidade. A privacidade pode ser entendida como o conjunto de informações acerca do indivíduo que do qual ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições, sem a isso ser legalmente sujeito [5].

Estes conceitos assumem nuances específicas em redes sociais *online*. No que diz respeito à integridade, a grande parte das redes sociais permite que apenas o dono da conta utilizada para autenticação no sistema possa alterar ou excluir dados. Essas permissões não podem ser passadas adiante para demais usuários da rede, tornando difícil a alteração não autorizada dos dados. Desse modo, quanto à integridade, não há uma preocupação tão grande por parte da maioria dos mecanismos de controle de acesso das redes sociais quanto à modificação ou exclusão de dados de um usuário feita por um usuário indevido, pois para isso se necessitaria saber o *login* e senha do usuário de uma conta, para assim se autenticar no sistema e fazer alterações não autorizadas [27]. Deve-se entender que estes problemas podem ser extrapolados para todo e qualquer acesso informatizado a dados. Entretanto, focamos neste trabalho apenas nas redes sociais.

Quanto à confidencialidade das informações pessoais contidas nos perfis de usuários, a maioria das redes usa um mecanismo baseado no nível de relacionamento que um usuário possui com a pessoa que acessa o dado. Em algumas redes, como o Facebook, o nível de relacionamento é dividido em, por exemplo, Todos, Amigo de Amigo, Amigo ou ainda alguma lista personalizada. O dado também pode ser marcado como privado, dando acesso apenas ao dono da conta. Esse mecanismo é bastante popular, pois proporciona um bom balanceamento entre flexibilidade e facilidade de uso e consegue capturar certo nível de confiança que um usuário possui para com aqueles que fazem parte da rede [27].

Compartilhar grandes quantidades de informação (incluindo textos, fotos e qualquer outro tipo de conteúdo) traz problemas de segurança e privacidade para usuários de redes sociais [33]. O tema de privacidade das informações tem recebido atenção crescente. 25% dos Americanos consideram-se vítimas pelo fato da privacidade de suas informações ter sido violada [9].

Uma discussão válida é se pessoas que compartilham tantas informações efetivamente têm alguma expectativa de privacidade. Deve-se entender que o objetivo do trabalho é avaliar o que a ferramenta oferece em termos de proteção e segurança dos dados para que o usuário possa facilmente decidir em que nível ele quer proteger suas informações. Concordamos que há uma questão humana, mas que não tira o papel da tecnologia em auxiliar o usuário. Este conceito pode ser visto explicitamente em [38], onde pode ser visto que os alunos de um curso de Farmácia passaram a utilizar melhor as configurações de segurança depois de conhecer as políticas correspondentes.

Muitas pessoas além de amigos e conhecidos estão interessadas em informações que as pessoas postam em redes sociais. Ladrões de identidade, de informações, perseguidores e corporações estão buscando vantagem competitiva usando redes sociais para reunir informações sobre consumidores. Neste cenário, tem-se a violação da propriedade autenticidade, quando uma pessoa se faz passar por outra, ou seja, o emissor de uma informação não é quem diz ser. Neste mesmo cenário, pode-se ainda ter violação de outras propriedades, como a legalidade, pois o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos ou ainda da disponibilidade, pois a informação pode não estar sempre disponível para uso quando usuários autorizados necessitarem [28].

Organizações que operam redes sociais estão coletando uma variedade de dados sobre seus usuários tanto para personalizar seus serviços quanto para vendê-las a anunciantes, conforme anunciado na própria política de dados do Facebook [12]. A preocupação com vazamento de informações e violação de segurança e privacidade das mesmas tem crescido em ambientes de redes sociais [15].

Algumas pessoas podem argumentar que ninguém lê o contrato de licença e que isso daria direitos ao Facebook, existindo então uma autorização tácita. Este é um ponto interessante e a discussão aqui é se isso está explícito e claro na interface para o usuário. Entendemos que há uma diferença entre não fazer por não saber e não fazer sabendo das configurações, mas optando-se por não utilizar e o trabalho procura investigar o primeiro aspecto apenas.

Na próxima seção os principais resultados são apresentados.

IV. ANÁLISE E DISCUSSÃO DA PROPOSTA DE SEGURANÇA DO FACEBOOK

Nesta seção, apresentamos a análise da interface do Facebook, realizada utilizando o MIS, indicando a proposta do projetista para segurança da informação nessa rede social, bem como as estratégias adotadas por ele.

A avaliação foi realizada no período de nove dias (entre 06/09/2014 e 15/09/2014) e foi conduzida por dois autores desse trabalho, sendo que um deles já havia realizado outras avaliações de interface no contexto de softwares sociais utilizando o método em questão [3].

O escopo foi limitado à versão em Português do Brasil do Facebook e às seguintes tarefas: (1) efetuar *login* e senha; (2) visualizar um conteúdo na linha do tempo; (3) visualizar foto; (4) comentar conteúdo de um *post*; (5) publicar um post na linha do tempo; (6) configurar privacidade da conta; (7) configurar segurança da conta e (8) conversar através do *chat*.

A escolha dos cenários se deu por estes serem diretamente relacionados às propriedades de segurança da informação no Facebook. As Figuras 1, 2 e 3, apresentadas a seguir, mostram exemplos dos signos inspecionados. Vale ressaltar que estão destacados em cada figura aspectos da interface que evidenciam o que será apresentado como proposta de segurança do projetista.

Para a apreciação dos signos metalinguísticos, foram analisados o *help* do sistema, os sub-tópicos *login* e senha, privacidade e dados pessoais. A Figura 1 mostra um exemplo de signo metalinguístico inspecionado no Facebook que contém instruções ao usuário sobre como remover uma marcação de uma foto ou publicação em que ele foi marcado.

Os signos estáticos, por sua vez, foram analisados a partir dos elementos que compõem a linha do tempo, o *feed* de notícias, o álbum de fotos, a configuração de privacidade e as mensagens instantâneas entre os usuários (bate-papo). A Figura 2 mostra um exemplo de signo estático inspecionado que contém elementos de interface que indicam a possibilidade de publicar um comentário, foto ou marcar em um local.

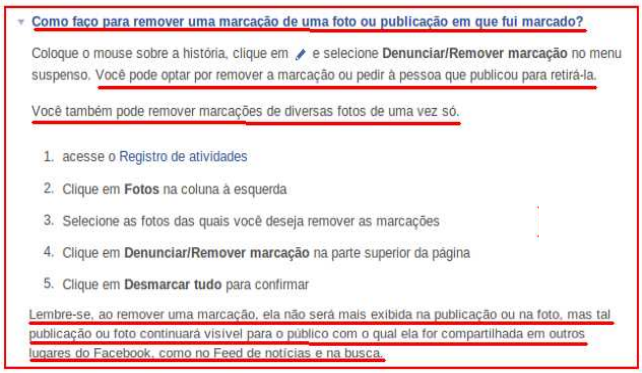

Fig. 1. Evidência de avaliação de signo metalinguístico.

Fig. 2. Evidência de avaliação de signo estático.

Finalmente, os signos dinâmicos foram apreciados através da interação com os recursos propostos para o compartilhamento de conteúdo, comunicação entre usuários e configurações de privacidade. A Figura 3 mostra um exemplo de signo dinâmico inspecionado no Facebook que permite configurar a visibilidade de publicação de um conteúdo.

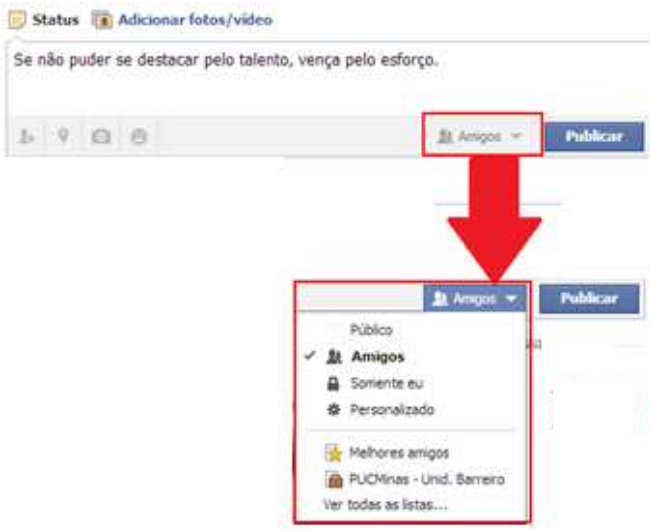

Fig. 3. Evidência de avaliação de signo dinâmico.

Os resultados alcançados com a aplicação do MIS e a junção das três metamensagens correspondentes à avaliação de símbolos estáticos, dinâmicos e metalinguísticos em uma mensagem final serão apresentados na próxima seção.

A. Proposta de Segurança da Informação do Facebook

A partir da inspeção para identificar a metamensagem do sistema, verificou-se que o propósito do projetista do Facebook é oferecer aos seus usuários um espaço onde seja possível realizar compartilhamento de conteúdos (como textos, vídeos, mensagens e imagens) e interação com outras pessoas.

O sistema dispõe de políticas e termos de uso que, conforme relatado pelo próprio projetista em sua metamensagem, devem ser seguidas porque, *"uma vez que o Facebook oferece às pessoas ao redor do mundo o poder de publicar suas próprias histórias, ver o mundo pelos olhos de muitas outras e conectar-se e compartilhar onde quer que elas estejam. A conversa que ocorre no Facebook – e as opiniões expressas aqui – reflete a diversidade das pessoas que usam o Facebook. Para equilibrar as necessidades e os interesses de uma população global, o Facebook protege a expressão que atende aos padrões da comunidade descritos nesta página"*.

Qualquer pessoa que possui e-mail e aceitar os termos e políticas pode criar uma conta no Facebook e começar a utilizar seus serviços. Ao criar um perfil, o usuário pode disponibilizar informações referentes a: (1) Trabalho e Educação; (2) Residência; (3) Relacionamentos (i.e., se você está solteiro, namorando, noivo ou separado); (4) Família (i.e., quem são seus familiares que estão no Facebook e qual o seu grau de parentesco entre eles); (5) Contatos (i.e., e-mails e telefones); entre outras informações (e.g., programas de TV, músicas, filmes e livros preferidos). Além disso, é possível disponibilizar uma imagem, cujo objetivo é identificar visualmente o proprietário do perfil. Dessas informações, o

projetista exige apenas que o usuário informe um nome identificador, que será utilizado para representá-lo.

Para que a interação entre os membros aconteça, o projetista do Facebook oferece um recurso de busca e localização de pessoas e um sistema de recomendação. Para iniciar uma amizade com outro membro, o proprietário do perfil tem duas opções: (1) enviar uma solicitação de amizade para alguém que pode aceitá-la ou não ou (2) aceitar a solicitação de amizade enviada por outro membro. Pensando em organizar os amigos que o usuário possui em seu perfil, o projetista oferece a possibilidade de agrupá-los em listas ou ainda especificar algum possível grau de parentesco.

Os principais recursos oferecidos para interação e compartilhamento de conteúdo entre o proprietário do perfil e seus amigos são *feeds* de notícias (ou mural), mensagens instantâneas (ou *chat*), eventos e grupos. Em relação ao *feed* de notícias, o usuário pode publicar conteúdo no próprio mural e/ou no mural de um amigo, neste último caso, desde que ele tenha essa permissão. O compartilhamento pode ser feito através de texto, imagem e/ou vídeo. Além disso, é possível incluir informações como data, localização ou mesmo marcar amigos.

Identificada a metamensagem do Facebook para seus usuários e considerando as propriedades de segurança da informação, foi possível verificar que o projetista endereça aspectos de segurança em sua interface, com o objetivo de apoiar a interação social segura de seus membros.

Dentre as decisões do projetista, relacionadas com a segurança, destaca-se o controle sobre a exibição do conteúdo compartilhado no perfil de um usuário. A visibilidade das publicações no mural, bem como das informações pessoais, fica ao critério do proprietário do perfil. Ele deve decidir se esse conteúdo é publico; restrito a amigos; privado (i.e., visível apenas ao dono do perfil) ou personalizado. Dessa forma, se o conteúdo publicado não é privado, seus amigos podem curtir, comentar e até mesmo compartilhar com outras pessoas. É importante ressaltar que o usuário consegue controlar apenas o que é visível pelo seu perfil e não pelo perfil de amigos.

Outra decisão relevante referente à segurança é a possibilidade de recusar ou aceitar solicitações de amizade. Dessa forma, o usuário consegue controlar quem tem acesso a seu perfil, o que não acontece em outras redes, como o Google+ e o Tweeter. O Facebook permite ainda configurar permissões sobre marcações e publicações feitas por terceiros em um perfil. Nesse caso, antes da publicação ser exibida no mural, o proprietário do perfil decide se o conteúdo deve ou não ficar visível em sua página. Entretanto, mesmo não autorizando a exibição, o conteúdo pode ser visto no perfil de quem o criou.

Note-se que o Facebook permite denunciar para que a foto seja excluída para sempre. Entretanto, posto que haverá uma análise humana, o tempo entre a publicação e a solução da denuncia é suficiente para propagação da informação.

Finalmente, em termos de disponibilidade, com o intuito de garantir uma boa socialização entre os usuários que mantêm contato através do Facebook, o projetista notifica cada membro sobre as atualizações que ocorrem em seu perfil. Por exemplo, quando uma solicitação de amizade ou uma mensagem é enviada ao membro, ou ainda, quando alguém compartilha, comenta ou curte seu *feed* de notícias, o usuário recebe uma notificação em tempo real para que tenha a oportunidade de fornecer um *feedback* para a pessoa ou grupo que interagiu com ele (e.g., responder uma mensagem, curtir um conteúdo, aceitar uma solicitação de amizade).

Identificada a proposta do projetista em relação à segurança no Facebook, na próxima seção são apresentadas as estratégias adotadas para prover essa propriedade no sistema.

B. Estratégias de Segurança da Informação Identificadas

A partir da proposta de segurança do Facebook, identificada com o MIS, foi possível constatar que o projetista faz uso de estratégias que consideram os pilares da segurança da informação apresentados na seção III B. A Tabela 1 apresenta as estratégias identificadas e que estão alinhadas com as propriedades de segurança apresentadas anteriormente, bem como as decisões do projetista (apontadas pelo MIS) que evidenciam essas estratégias no Facebook. Vale ressaltar que, em alguns casos, uma mesma estratégia reflete em diferentes decisões do projetista. Em seguida, serão apresentados alguns exemplos de como estas estratégias foram implementadas no Facebook.

TABELA 1
ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO DO FACEBOOK

Estratégia / Propriedade da Segurança da Informação	Decisões do Projetista	Justificativa no Contexto de Segurança da Informação
E1 – Autenticidade	D1 – *Login* e Senha para acesso ao Facebook	Identifica o usuário que está utilizando o Facebook. Garante que o usuário é realmente quem afirma ser, por exemplo, que o usuário foi quem criou a conta e tem autorização de acesso (mas não necessariamente se ele é quem diz ser no seu perfil).
	D2 – Aprovar solicitação de amizade	Garante ao usuário a possibilidade de escolher com quem ele deseja se relacionar (i.e., comunicar/trocar informações) na rede social. Dessa forma, o usuário consegue verificar a fonte e/ou destinatário de conteúdos que serão compartilhados/visualizados a partir do seu perfil.
E2 – Confidencialidade	D3 – Definição da visibilidade/privacidade do conteúdo no perfil	Garante ao usuário controlar quem tem acesso às suas informações pessoais e compartilhamentos. Em outras palavras o usuário define o grau de sigilo de cada informação
E3 – Disponibilidade	D4 – Notificação de atualizações no perfil em tempo real	Disponibiliza em tempo real notificações sobre atualizações que ocorreram no perfil do usuário (e.g., solicitações de amizade, publicações no mural). Essa decisão permite que o usuário forneça um *feedback* para a pessoa ou grupo que interagiu com ele
E4 – Integridade	D5 – Analisar marcações de terceiro antes de exibi-las no perfil do usuário	Garante ao usuário a possibilidade de decidir se é conveniente ou não publicar conteúdos em seu perfil – não submetidos originalmente por ele (i.e., compartilhado por um amigo) - e verificar, antes da publicação, se o conteúdo é integro (i.e., se não foi alterado e/ou manipulado de forma indevida)
E5 – Legalidade	D6 – Denunciar conteúdo impróprio	Permite ao usuário denunciar conteúdos que não obedecem as politicas de uso, segurança e privacidade do Facebook. Dessa forma, busca-se garantir que o conteúdo e comportamento adotado dentro da rede social sejam conduzidos por normas/leis.

A Figura 4 exibe um exemplo de implementação da estratégia identificada como D2 na Tabela 1, relacionada à propriedade de segurança de informação Autenticidade. Essa decisão do projetista está relacionada à propriedade Autenticidade porque o usuário consegue verificar e identificar quem está enviando convites de solicitação de amizade.

Fig. 4. Evidência da Decisão do Projetista D2.

A Figura 5 exibe um exemplo de implementação da estratégia identificada como D4 na Tabela 1, relacionada à propriedade de segurança de informação Disponibilidade. A Figura 5 mostra como o usuário pode visualizar em tempo real notificações sobre atualizações que ocorreram em seu perfil. Desta maneira, o usuário pode fornecer *feedback* para a pessoa ou grupo que interagiu com ele.

Fig. 5. Evidência da Decisão do Projetista D4.

A Figura 6 exibe um exemplo de implementação da estratégia identificada como D6 na Tabela 1, relacionada à propriedade de segurança de informação Legalidade. A Figura 6 mostra como o usuário pode denunciar conteúdos que não obedecem as politicas de uso, segurança e privacidade do Facebook. Dessa forma, busca-se garantir que o conteúdo e comportamento adotado dentro da rede social seja conduzido por normas/leis. A Figura 6 evidencia que há a possibilidade de decidir, seja por solicitação direta ou recomendação se o usuário deseja ou não manter o contato na sua rede.

Fig. 6. Evidência da Decisão do Projetista D6.

Finalizada essa etapa de identificação de estratégias, foi possível verificar que o projetista oferece recursos que encorajam e possibilitam a segurança da informação entre os membros do Facebook e que, para isto, ele adota algumas estratégias de segurança (i.e., propriedades) consideradas relevantes no contexto do projeto de interface para sistemas que visam promover a interação social mediada pelo computador de forma segura.

Conforme indicado anteriormente, o objetivo principal desse trabalho foi caracterizar as estratégias de segurança de informação comunicadas na interface do Facebook. Entretanto, de forma complementar, buscamos identificar os potenciais problemas (rupturas) que poderiam ser vivenciados pelos usuários dessa rede social relacionados à segurança. Na próxima seção, esses resultados são sumarizados e discutidos.

C. Rupturas Encontradas

Nesta seção, são descritas as principais rupturas (RP) identificadas pelo MIS e discutido o potencial impacto que cada uma delas pode ter na segurança do usuário no Facebook. Vale destacar que os argumentos apresentados para justificar os potenciais problemas foram fundamentados no trabalho realizado por [26] que discute os impactos da violação de segurança em sistemas online.

RP1. Falta de clareza para acesso a configurações de segurança. Há uma seção no Facebook denominada "Como conectar" que possui um conjunto de perguntas relacionadas diretamente às configurações de segurança e privacidade. Logo, o atual nome da seção é incoerente com o conteúdo das perguntas, uma vez que não sugere que nesse espaço é possível encontrar informações referentes às configurações de segurança. Essa ruptura pode impactar na segurança do usuário porque ao não perceber que a rede disponibiliza recursos que auxiliam nessas configurações, o usuário pode deixar realizar uma configuração e/ou esclarecer uma dúvida relacionada à segurança no Facebook e, consequentemente, ficar vulnerável nessa rede social, o que causaria uma possível violação de confidencialidade ou até mesmo integridade.

RP2. Utilização de termos ambíguos. O projetista utiliza termos ambíguos para expressar, na versão em português do sistema, os mesmos conceitos ou funcionalidades. Um exemplo desta ambiguidade seria o uso do termo "Política de Privacidade" para acessar configurações de segurança, que pode ser considerado um termo mais amplo que o utilizado. Essas ambiguidades podem dificultar, ou até mesmo inviabilizar a identificação e uso dos recursos disponíveis dentro do Facebook para configurar aspectos de segurança na rede, causando possíveis violações de confidencialidade.

RP3. Número excessivo de passos para acesso à Ajuda em relação às configurações de segurança. Caso o usuário tenha dúvidas e precise acionar a ajuda do Facebook para esclarecimentos sobre a segurança na rede, ele se depara com um número excessivo de passos para chegar à informação desejada (pelo menos 07 cliques). Isso é problema porque viola um principio básico de usabilidade de interface, o reconhecimento ao invés de memorização [20][23]. Neste caso, o usuário precisa memorizar o caminho para acesso a informação, que por ser longo pode inviabilizar essa busca, comprometendo o uso correto das configurações, em caso de dúvidas não esclarecidas.

RP4. Limitação nas configurações de visibilidade do conteúdo. Embora o Facebook ofereça um mecanismo para que o usuário possa configurar a visibilidade do conteúdo exibido em seu perfil (e.g., textos, fotos e vídeos publicados em seu mural), não existe uma forma explicita de controlar o conteúdo exibido no mural de um amigo, caso esse conteúdo faça referência a outro usuário. Essa decisão impacta na segurança, uma vez que, uma pessoa pode ser exposta por outra, mesmo que isso não seja intencional, causando quebra de confidencialidade das informações pessoais.

RP5. Restrição à denúncia apenas a usuários que possuem conta no Facebook. O Facebook oferece a possibilidade de denunciar perfis que não respeitam suas regras de utilização (e.g., perfis falsos). Entretanto, no caso de um perfil falso, essa denúncia está restrita apenas a usuários que possuem conta no Facebook. Isso porque, embora o Facebook disponibilize instruções para denunciar uma conta falsa, através da página de ajuda "Como faço para denunciar uma conta falsa?" (https://www.facebook.com/help/167722253287296), as opções listadas estão visíveis apenas para usuários conectados (i.e., que possuem conta) no Facebook. Em outras palavras, se o usuário que teve seu perfil falsificado, acessar a referida página, a partir de seu endereço no Facebook, embora ele consiga visualizar o perfil, a opção para denúncia não está disponível. Nesse caso, poderá haver o uso indevido do nome e dos dados de uma pessoa que teve um perfil falso criado em seu nome, mas que não possui uma conta oficial no Facebook.

V. CONCLUSÕES FINAIS E TRABALHOS FUTUROS

Neste trabalho, a questão de pesquisa consistiu em analisar como o projetista comunica através da interface do Facebook as propriedades da segurança da informação dentro do contexto de rede social.

Nesse sentido, foi possível concluir que de acordo com a metamensagem final, o projetista do Facebook

buscou potencializar a segurança da informação nesse sistema, incorporando em sua interface, de forma complementar, as propriedades consideradas "os pilares da segurança". Entretanto, algumas propriedades foram mais evidenciadas (e.g., a confidencialidade) do que outras. Por exemplo, não é possível identificar informações que permitem ao usuário encontrar, facilmente, os termos de uso do Facebook, percebe-se então, que a propriedade da segurança legalidade é baixa ou pouco explorada.

Assim, podemos entender que em uma rede social, por exemplo, para o projetista, seria mais importante a confidencialidade, do que a disponibilidade, mas o que não indica que ele não a aborde, mas não evidencia com tantos recursos.

Em termos de contribuições, apesar de apresentar um estudo de caso no Facebook, a apreciação realizada se faz relevante tanto em termos práticos, quanto científicos/metodológicos para a área de Interação Humano Computador (IHC) e Segurança da Informação.

Em aspectos práticos, os resultados contribuem para a melhoria e/ou desenvolvimento de soluções que potencializem a segurança da informação nas redes sociais, isso porque o artigo oferece uma perspectiva sobre as estratégias de segurança da informação comunicadas na interface do Facebook que podem ser adotadas em outras redes.

Em termos científicos/metodológicos, os resultados do MIS reforçam a aplicabilidade do método, devido à sua fundamentação teórica, para identificar as estratégias de design, comunicadas na interface, que visam potencializar determinadas qualidades de uso, neste caso, as estratégias de segurança da informação.

Note-se que neste momento, é impossível concluir se o Facebook é bom ou não em relação aos seus critérios. O escopo deste trabalho focou em apresentar o que existe de recursos e problemas do ponto de vista de um especialista em interação. Embora essa análise seja importante e necessária, nos permite identificar evidências que devem ser confirmadas por meio de uma triangulação feita com estudos com usuários. Logo entendemos que essa afirmação deveria ser feita após este estudo, como previsto nos trabalhos futuros.

Como proposta de trabalho futuro, pretende-se avaliar sob o ponto de vista do usuário, através do Método de Avaliação de Comunicabilidade (MAC), qual a sua percepção acerca das propriedades de segurança da informação e se de fato as estratégias do Facebook apoiam os usuários nesse aspecto.

Além disso, outro ponto a ser investigado é a possibilidade de identificar signos na interface que permitem classificar as possibilidades de segurança da informação oferecidas pelas redes sociais online. Isso ajudaria no projeto e avaliação de outras redes, como por exemplo, o Instagram. Assim, poderemos demonstrar que nossa abordagem é aplicável a várias redes e não só uma peculiaridade do Facebook.

REFERÊNCIAS

[1] A. Albesher and T.Alhussain. "Privacy and security issues in social networks: an evaluation of Facebook". *Proceedings of the 2013 International Conference on Information Systems and Design of Communication (ISDOC)*, pp. 7-10, 2013.

[2] A. E. Albuquerque Júnior and E. M dos Santos. "Análise das Publicações Brasileiras sobre Segurança da Informação sob a Ótica Social em Periódicos Científicos entre 2004 e 2013". In: *XXXVIII Encontro da ANPAD, ENANPAD*, 2014, Rio de Janeiro.

[3] G. A. R . Barbosa, G. E. Santos and V. M. Pereira. "Caracterização Qualitativa da Sociabilidade no Facebook". In *Proceedings of XII Simpósio de Fatores Humanos em Sistemas Computacionais - IHC* 2013, Manaus, AM. .

[4] W. Binden, M. Jormae, Z. Zain and J. Ibrahim. "Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks". *International Journal of Scientific and Research Publications*, Volume 4, Issue 1, Janeiro de 2014.

[5] C. E. B. A. Bragança, E. M. Luciano, M. G. Testa. "Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da priacidade percebida pelos profissionais". *XXXIV Encontro da ANPAD (ENANPAD)*, 2010.

[6] CERT.BR. "Estatísticas dos Incidentes Reportados ao CERT.br. 1999 a junho de 2013". Disponível em: http://www.cert.br/stats/incidentes. Acesso em 02/06/2015.

[7] COMSCORE. "Facebook Blasts into Top Position in Brazilian Social Networking Market Following Year of Tremendous Growth". 2012. Disponível em <http://goo.gl/TcXcM>. Acesso em 02/06/2015.

[8] F. Coutinho, R. O. Prates, L. Chaimowicz. "An analysis of information conveyed through audio in an fps game and its impact on deaf players experience". In: *IEEE. Games and Digital Entertainment (SBGAMES)*, 2011.

[9] A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh, J. Minj. "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook". In *3rd IEEE International Advance Computing Conference (IACC)*. 2013.

[10] F. Duarte, C. Quandt. "O tempo das redes in redes urbanas". São Paulo, Brasil: Editora Perspectiva, 2008.

[11] N. B. Ellison, C. Steinfield and C. Lampe. "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites". *Journal of Computer Mediated Communication*, 12(4), 1143-1168, 2007.

[12] Facebook. Política de Dados. Disponível em https://www.facebook.com/about/privacy/. Acesso em 19/10/2015.

[13] A. A. Hasib. "Threats of online social networks". Helsinki , Finland : Helsinki University of Technology. 2008.

[14] IDEC - Instituto Brasileiro de Defesa do Consumidor . 2012. "Pesquisa Quem vê seu perfil?" Disponível em http://www.idec.org.br/uploads/revistas_materias/pdfs/172-pesquisa-redes-sociais1.pdf. Acesso em 02/06/2015.

[15] M. R. Khayyambashi and F. S. Rizi. "An approach for detecting profile cloning in online social networks". In *7th International Conference on e-commerce on developing countries with focus on e-security*. 2013.

[16] ITSMF. "Fundamentos do Gerenciamento de Serviços em TI baseados no ITIL". Holanda: Van Haren Publishing, 2006.

[17] K. Malagi, A. Angadi and K. Gull. "A Survey on Security Issues and Concerns to Social Networks". I*nternational Journal of Science and Research (IJSR)*, India Online ISSN: 2319-7064 Volume 2 Issue 5, Maio 2013.

[18] E. S. Martins, F. J. V. Lucas and R. C. S. Vasconcelos. "Segurança da informação nas redes sociais". *Revista Sinergia*, São Paulo, v. 15, n. 4, p. 272-278, out./dez. 2014.

[19] C. Ngeno, P. Zavarsky, D. Lindskog and R. Ruhl. "User's Perspective: Privacy and Security of Information on Social Networks". In *IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust*. 2010.

[20] J. Nielsen. "Heuristic evaluation". In: J. Nielsen e R. L. Mack (Eds.) *Usability inspection methods*. New York: John Wiley & Sons, 1994. p. 25–62.

[21] C. S. Peirce. “The Essential Peirce”. Indiana University Press, Bloomington, 1992.
[22] R. O. Prates, S. D. J. Barbosa. “Introdução à Teoria e Prática da Interação Humano Computador fundamentada na Engenharia Semiótica”. *Jornada de Atualização em Informática (JAI)*, Congresso da SBC, 2007.
[23] R. O. Prates e S. Barbosa. Avaliação de Interfaces de Usuário– Conceitos e Métodos. In:*Anais do XXIII Congresso Nacional da Sociedade Brasileira de Computação. XXII Jornadas de Atualização em Informática (JAI)*. SBC 2003.
[24] J. Preece. “Online communities: Usability, Sociability, Theory and Methods”. In R. Earnshaw, R. Guedj, A. van Dam and T. Vince (Eds) *Frontiers of Human-Centred Computing, Online Communities and Virtual Environmen*ts. 2001
[25] S. D. S. Reis and R. O. Prates. “Applicability of the semiotic inspection method: a systematic literature review”. In Proce*edings of the X Symposium on Human Factors in Computing Systems and V Latin American Conference on Human Computer Interaction, IHC & CLIHC*, 2011.
[26] A. Santos and A. Andrade. “Portais de bibliotecas sistemas de avaliação de qualidade dos serviços”. *Información, cultura y sociedad*, no 22, 2010.
[27] V. S. Santos, E. Porto and B. “Alturas. Análise de mecanismos de controle de acesso nas redes”. *Revista Portuguesa e Brasileira de Gestão*, Vol. 9, No. 3, pp.50-60, ISSN: 1645-4464, 2010.
[28] M. Sêmola. “Gestão da Segurança da Informação: Uma visão executiva”. 5. ed. Rio de Janeiro: Campus-Elsevier, 2003.
[29] J. C. R. da Silva; G. A. R. Barbosa. “Estratégias de gamificação como fator motivacional para o uso de aplicativos móveis educacionais:Um estudo de caso do aplicativo duolingo”. *Simpósio Mineiro de Engenharia de Software (SMES)*. Belo Horizonte, Minas Gerais, 2014.
[30] M. C. F. Silva and A. Oliveira. “Marketing communication strategies for the corporate website of promenade champagnat: Using MIS at tourism”. *Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais*, 2014.
[31] C. S. de Souza. “The semiotic engineering of human-computer interaction”. MIT Press, 2005.
[32] C. S. de Souza, C. S. Leitão, R. O. Prates and E. J. da Silva. “The semiotic inspection method”. In *Proceedings of VII Brazilian symposium on Human factors in computing systems (IHC '06)*. ACM, New York, NY, USA, 148-157, 2006.
[33] A. S. Yuksel, M. E. Yuksel and A. H. Zaim. “An Approach for Protecting Privacy on Social Networks”. *Fifth International Conference on Systems and Networks Communications.* 2010.
[34] R. A.Zilpelwar, R. K. Bedi, and V. M. Wadhai. An Overview of Privacy and Security in SNS. International Journal of P2P Network Trends and Technology- Volume2 Issue1- 2012.
[35] N. B. X. Silva.; W. J. de Araújo and P. M. de Azevedo. 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. Revista Ibero-americana de Ciência da Informação, v. 6, n. 2, p. 37-55, ago./dez. 2013
[36] J. Preece. Sociability and usability in online communities: Determining and measuring success. Behaviour & Information Technology. Behaviour & Information Technology 20, 5, (2001), 347–356.
[37] R. Pereira; M. C. C. Baranauskas and S. R. P. da Silva. Softwares sociais: uma visão orientada a valores. In Proc. of the IX Symposium on Human Factors in Computing Systems, IHC ’10, (2010), 149-158.
[38] J. Williams; C. Feild and K. James. The Effects of a Social Media Policy on Pharmacy Students’ Facebook Security Settings. American Journal of Pharmaceutical Education, v. 75, n.9, 2011.
[39]