# AMEAÇAS À SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

**Autores**: Francisco Gabriel Teixeira Marinho[(1)], Evelym Vasconcelos Moraes dos Santos[(1)], Ramon Breno dos Santos Rodrigues[(1)], Odette Mestrinho Passos[(1)]

**Filiação/Endereço/Email:** 1. Instituto de Ciências Exatas e Tecnologia – Universidade Federal do Amazonas. Rua Nossa Senhora do Rosário, 3683 – Tiradentes – Itacoatiara/AM, fgtemarinho@gmail.com, evelym.vasconcelos@gmail.com, ramonicet@gmail.com, odette@ufam.edu.br

**Resumo**: O valor da informação se mostra como um fator de sucesso para muitas organizações, pois as mesmas investem em equipamentos de segurança e softwares sofisticados com um intuito de fortalecer a segurança de suas informações, mas mesmo assim, enfrentam uma grande ameaça bastante recorrente: os ataques da Engenharia Social, realizados por indivíduos que buscam romper barreiras de segurança para ganhos próprios. A segurança da informação busca preservar o valor da informação, desta maneira, a Engenharia Social torna-se uma adversária muito perigosa que pode causar danos a ela. Este trabalho teve como objetivo descrever os resultados de uma investigação sobre as principais ameaças a segurança da informação nas organizações, além de expor quais são as principais técnicas utilizadas pelos engenheiros sociais. A metodologia científica adotada para o desenvolvimento desta pesquisa foi baseada em um estudo denominado mapeamento sistemático que fornece uma visão geral de uma área de pesquisa, identificando a quantidade, os resultados disponíveis, além das frequências de publicações ao longo do tempo para identificar tendências. Os resultados apontam dois principais motivos que ameaçam a segurança da informação: a Engenharia Social e a vulnerabilidade quanto aos princípios de disponibilidade, confidencialidade e integridade. As técnicas mais utilizadas pela engenharia social é a denominada *Phishing*, que significa uma forma de enviar mensagens falsificadas e a coleta de dados via internet para realizar os ataques cibernéticos.

**Palavras-chave:** Engenharia Social; Segurança da Informação; Organização.

## Introdução

A engenharia é a habilidade de criar, inventar e manipular algo por intermédio de uma técnica. Social é tudo aquilo que é relativo a forças externas ao indivíduo, provenientes do meio onde ele vive, determinando assim grande parte do seu comportamento (BRAGA, 2010). A partir desses conceitos, pode-se definir engenharia social como uma técnica de utilizar a influência e a habilidade de enganar pessoas para persuadi-las a fim de obter informações sigilosas com ou sem o uso de recursos tecnológicos (MITNICK, 2005; SILVA *et al.*, 2012).

Para Silva (2012), a Engenharia social é a aplicação de conhecimentos empíricos e científicos de um modo sociável de acordo com as necessidades humanas para obter informações. Pode-se afirmar também que é a arte de manipular as pessoas visando contornar dispositivos de segurança (CARVALHO e GALVÃO, 2015).

O engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia. Assim sendo, a Engenharia Social é um dos meios mais utilizados para obter informações importantes porque explora muito as falhas do fator humano (MITNICK, 2005).

Os engenheiros sociais são bastante conhecidos como *Hackers*, todavia, estudiosos dessa área dividem opiniões ao conceituarem esses indivíduos no que se refere à finalidade com que eles realizam essa prática, pois quando a Engenharia Social é realizada com o intuito de obtenção de conhecimento, visando descobrir vulnerabilidades para aprimorar os sistemas de segurança, o indivíduo que a pratica é denominado de *hacker*, mas quando a finalidade é acessar informações para obter benefícios próprios, prejudicando indivíduos ou organizações, o indivíduo é chamado de *cracker* (FILHO, 2010).

*Hackers* são pessoas com conhecimentos técnicos sofisticados que as tornam capazes de invadir sistemas de computadores, não com a intenção de provocar danos a usuários ou fabricantes. Os *crackers* também possuem conhecimentos superiores nessa área, mas são chamados de "piratas eletrônicos", pois não realizam essas atividades para fins éticos, eles quebram os dispositivos de segurança de redes de computadores para roubar informações estratégicas ou obter algum tipo de vantagem. Por meio de técnicas de Engenharia Social, eles conseguem "arrancar" informações das pessoas, facilitando assim muitos ataques. Isso pode causar grandes danos à segurança da informação de uma organização (FILHO, 2010; SILVA *et al.*, 2012).

A engenharia social é uma ameaça que não necessita de conhecimentos técnicos e nem de grandes investimentos para a proteção da segurança da informação, necessita de conhecimentos dos métodos e técnicas de como se defender de um engenheiro social que tem como objetivo acessar informações sigilosas (CARVALHO e GALVÃO, 2015). Contudo, a motivação para a criação deste trabalho é compreender como é realizada a engenharia social nas organizações e mostrar que esta é a principal ameaça à segurança da informação nas organizações.

A metodologia de pesquisa adotada neste trabalho, para coletar as informações de forma a cumprir o objetivo, está fundamentado nos princípios da Engenharia de Software Experimental que se baseia na condução de um estudo secundário: Mapeamento Sistemático (MS).

O MS fornece uma visão geral de uma área de pesquisa, identificando a quantidade, os tipos de pesquisas realizadas, os resultados disponíveis, além das frequências de publicações ao longo do tempo para identificar tendências (PETERSEN *et al.*, 2008).

Assim sendo, este artigo tem como objetivo apresentar o tema Engenharia Social, bem como as principais ameaças à segurança da informação, além de mostrar também quais são as técnicas mais utilizadas pelos engenheiros sociais.

Pode-se perceber pelos resultados obtidos que uma das principais ameaças na segurança da informação das organizações não está no conjunto de ferramentas tecnológicas utilizadas para invadir sistemas e obter informações, mas sim no fator humano, na maneira de persuadir o próximo ou de ser influenciado a liberar informações.

Como trabalhos relacionados, podemos citar o trabalho de Silva (2012) que buscou questionar se as pessoas que manipulam sistemas de segurança têm atributos para fazer isso da melhor forma possível, além de mostrar que além de equipamentos tecnológicos de ataque, a capacidade humana de persuadir o próximo para se conseguir o que quer é uma ameaça que pode trazer grandes danos à segurança da informação. A

metodologia utilizada foi a realização de pesquisas exploratórias orientadas por professores de administração e metodologia e desenvolvidas pelo autor em instituições de ensino e empresas utilizando questionário e observação pessoal. Como resultado, descobriu-se que funcionários mais novos são mais vulneráveis aos ataques e a Engenharia Social é o elo mais fraco da segurança de dados e informações confidenciais.

A sociedade da informação possui muitas vulnerabilidades devido a facilidade de veiculação das informações facilitada pela comunicação de redes digitais distribuídas, conforme foi exposto pela pesquisa de Coelho, Rasma e Morales (2013). O objetivo dessa pesquisa foi contribuir na identificação de regras e procedimentos com vistas à segurança da informação e apresentar uma revisão bibliográfica sobre o tema Engenharia Social. Para isso foi realizada um estudo exploratório de caráter qualitativo a partir de um levantamento bibliográfico. Com resultado, foram identificados regras e procedimentos que ajudam na prevenção de técnicas da Engenharia Social.

Com o objetivo de apresentar os resultados de análise sobre Engenharia Social, além das ameaças e cuidados aos funcionários das Agências Bancárias de Santarém e Itaituba, por intermédio de análises em artigos científicos, revistas, livros técnicos, sites especializados, e análises de questionários respondidos por funcionários das agências bancárias, o trabalho de Carvalho e Galvão (2015) concluiu que para se defender da engenharia social é necessário ter o conhecimento de métodos e técnicas de como se defender de um engenheiro social, e não de conhecimentos técnicos ou grandes investimentos para proteger a segurança da informação.

As pesquisas de Silva (2012) e Coelho, Rasma e Morales (2013) se assemelham a este artigo no que se refere a mostrar que a Engenharia Social é uma grande ameaça à segurança da informação, além de mostrar alguns procedimentos, todavia não mostram técnicas de engenharia social, utilizando o mapeamento sistemático. A pesquisa de Carvalho e Galvão (2015) se relacionada com este trabalho quando mostra que o conhecimento de técnicas de prevenção contra Engenharia Social é tão importante quanto grandes investimentos em equipamentos de segurança, mas utiliza uma metodologia diferente do mapeamento sistemático.

Segundo Marciano (2006), a segurança da informação é um domínio tecnológico, onde ferramentas e recursos tecnológicos são aplicados afim de buscar soluções para problemas gerados muitas vezes, com os recursos dessa mesma tecnologia. No contexto geral, ela está relacionada a práticas e controles adequados, formada por normas e procedimentos com intuito de preservar o valor da informação para um indivíduo ou uma organização. Ela preserva os ativos da informação, isto é, indivíduos, compostos tecnológicos, ou processos envolvidos no ciclo de vida da informação. Suas propriedades básicas são confidencialidade, integridade, autenticidade e disponibilidade.

## Métodos e Materiais

O MS foi baseado no *guidelines* desenvolvido por Kitchenham e Chartes (2007) e definido em três etapas: (a) Planejamento do Mapeamento: nesse passo, os objetivos da pesquisa são listados e o protocolo do mapeamento é definido; (b) Condução do Mapeamento: durante essa fase, as fontes para o mapeamento são selecionadas, os estudos são identificados, selecionados e avaliados de acordo com os critérios estabelecidos no protocolo do mapeamento e (c) Resultado do Mapeamento: nessa fase, os dados dos estudos são extraídos e sintetizados para serem publicados.

Na etapa do *Planejamento do Mapeamento Sistemático* foi definido o objetivo do estudo, as questões da pesquisa, a formulação da expressão de busca, além de definir os critérios de seleção de cada publicação e mencionar os procedimentos de extração dos dados.

- **Objetivo e Questões de Pesquisa**

O objetivo deste mapeamento sistemático é analisar publicações científicas com o propósito de investigar as principais ameaças às organizações causadas pela engenharia social com relação ao sucesso ou fracasso da segurança da informação do ponto de vista dos pesquisadores no contexto das organizações. Sendo assim, este MS busca respostas para as seguintes questões de pesquisa (QP):

**QP1:** Quais as principais ameaças à segurança da informação nas organizações?
**QP2:** Quais as técnicas utilizadas pela engenharia social?

- **Fontes e Expressão de Busca**

Os locais de buscas definidos para esta pesquisa foram feitos a partir da busca manual nos anais das conferências nacionais relacionadas à Segurança da Informação apoiada pela SBC (Sociedade Brasileira de Computação) que possui relação com o tema a ser pesquisado: Simpósio de Segurança da Informação e Sistemas Computacionais (SBSEG) e Simpósio Brasileiro de Sistemas de Informação (SBSI). Além disso, foram realizadas pesquisas no Google Acadêmico.

A busca foi restringida usando-se palavras-chave específicas para encontrar as publicações de interesse definidas de acordo com dois dos quatro aspectos indicados em Petersen *et al*. (2008): População e Intervenção.

- **População:** publicações que fazem referências a segurança da segurança da informação
  *Palavras-chave:* "segurança da informação" OU "hacker" OU "cracker"
- **Intervenção:** publicações que fazem referências a engenharia social:
  *Palavras-chave:* "engenharia social" OU "engenheiro social"

- **Critérios de Seleção**

Esta pesquisa se restringe à análise de publicações disponíveis até a data presente da execução do estudo. A seleção das publicações foi realizada em três etapas:

**(1)** Busca preliminar das publicações coletadas nas fontes definidas;
**(2)** Primeira Seleção: por meio de análise do título, o resumo e as palavras-chave e aplicando o critério de seleção "CS1: possuir informações sobre à segurança da informação nas organizações;
**(3)** Segunda Seleção: por meio da leitura completa das publicações e aplicando o critério de seleção "CS2: apresentar ameaças à segurança da informação fornecendo técnicas utilizadas pela Engenharia Social.

- **Procedimentos de Extração de Dados**

Foram extraídas informações de publicações relevantes para a pesquisa para serem registradas, conforme os campos abaixo, descritos na Tabela 1:

**Tabela 1 - Campos de coleta de dados**

| **A) Dados da publicação:** | |
|---|---|
| Título: | Indica o título do trabalho |
| Autor(es): | Nome dos autores |
| Fonte de Publicação: | Local de publicação |
| Ano da Publicação: | Ano de publicação |
| Resumo: | Texto contendo uma descrição do resumo |
| **B) Dados derivados do objetivo:** | |
| Engenharia Social: | Descrição da engenharia social mencionado na publicação |
| Principais ameaças à segurança da informação: | Descrição das ameaças sofridas pelas organizações no que se refere à segurança de suas informações |
| Técnicas utilizadas pela engenharia social: | Descrição de como são as técnicas utilizadas pelos engenheiros sociais para obter dados sigilosos de uma organização |

Na etapa da *Condução do Mapeamento Sistemático*, a execução do MS ocorreu entre os meses de Março e Junho de 2017, e as publicações foram selecionadas de acordo com os critérios estabelecidos no protocolo. Publicações duplicadas, inacessíveis ou indisponíveis na internet foram descartadas. Além disso, foram excluídas as publicações que claramente abordavam outros assuntos não relevantes para a pesquisa.

Foram investigados por buscas manuais os anais do SBSEG de 2009 a 2016, obtendo 14 publicações, e nos anais do SBSI de 2009 até 2016, obtendo 11 publicações. Nas buscas automáticas no Google Acadêmico foram reportadas 13 publicações.

Após a primeira análise, de acordo com o 1º filtro (leitura do título e resumo da publicação), 13 publicações foram selecionadas pelo critério CS1, como apresentado na Tabela 2. Do total das publicações que resultaram do 1º filtro, todas foram lidas na íntegra e ao final 8 publicações foram selecionadas por estarem de acordo com o critério CS2, como apresentado na Tabela 2. Para todas as 8 publicações (veja a Tabela 3) foram preenchidas as informações nos formulários de coleta de dados, conforme os dados definidos para extração de dados descritos no protocolo do MS.

**Tabela 2 - Publicações encontradas por etapa**

| Publicações Retornadas | Inicialmente | Após o 1º Filtro | Após o 2º Filtro |
|---|---|---|---|
| SBSEG | 14 | 0 | 0 |
| SBSI | 11 | 3 | 2 |
| Google Acadêmico | 13 | 10 | 6 |
| **TOTAL** | 38 | 13 | 8 |

## Resultados e Discussões

Com relação a última etapa *Resultado do Mapeamento*, foram relatados os resultados e discussões conforme as duas questões de pesquisas definidas.

- **Análise e Discussão da QP1**

Com relação à primeira questão de pesquisa "Quais as principais ameaças à segurança da informação nas organizações?", foi possível perceber que quase todas as publicações citam a Engenharia Social como principal ameaça à segurança da informação, como pode ser observado na Tabela 4.

**Tabela 3 - Publicações selecionadas após o 2º Filtro**

| ID | Título | Autores | Ano | Publicação | Fonte |
|---|---|---|---|---|---|
| [P01] | Engenharia Social: O Elo Mais Frágil da Segurança Nas Empresas | SILVA, C. | 2012 | Revista Eletrônica do Alto Vale do Itajaí | Google Acadêmico |
| [P02] | Engenharia Social: O Fator Humano Na Segurança Da Informação | SILVA, A. | 2010 | Coleção Meira Mattos: Revista das Ciências Militares | Google Acadêmico |
| [P03] | Engenharia Social: Uma Ameaça à Sociedade Da Informação | COELHO, C.; RASMA, E.; MORALES, G. | 2013 | Perspectivas online: Ciências Exatas e Engenharia | Google Acadêmico |
| [P04] | Engenharia Social: Uma Análise De Ameaças E Cuidados Aos Funcionários Das Agências Bancárias De Santarém E Itaituba – Pará | CARVALHO, C.; GALVÃO, A. | 2015 | Revista de Publicação Acadêmica da Pós-Graduação do IESPES | Google Acadêmico |
| [P05] | Engenharia Social e a Aleatoriedade na Escolha do Alvo | JUNIOR, J.; BARCAROLI, V. | 2016 | Tecnológica: Revista Científica | Google Acadêmico |
| [P06] | Engenharia Social: Uma análise sobre o ataque de *Phishing* | SILVEIRA, L.; REALAN, M.; AMARAL, E. | 2016 | Congresso Sul Brasileiro de Computação (SULCOMP) | Google Acadêmico |
| [P07] | Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico | MACHADO, C.; CABRAL, L.; SANTOS, J.; MOTTA, G. | 2009 | Anais do V Simpósio Brasileiro de Sistemas de Informação | SBSI |
| [P08] | O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e *Phishing* | ALENCAR, G.; LIMA, M.; FIRMO, A. | 2013 | Anais do IX Simpósio Brasileiro de Sistemas de Informação | SBSI |

**Tabela 4 – Resultados da QP1 identificadas nas publicações selecionadas**

| ID | Principais Ameaças à Segurança da Informação nas Organizações |
|---|---|
| [P01] | Engenharia Social e *Crackers* |
| [P02] | Engenharia Social e a vulnerabilidade quanto aos princípios de Disponibilidade, Confidencialidade e Integridade |
| [P03] | Engenharia Social e a vulnerabilidade quanto aos princípios de Disponibilidade, Confidencialidade e Integridade |
| [P04] | Engenharia Social, a vulnerabilidade quanto aos princípios de Disponibilidade, Confidencialidade e Integridade, *Hackers* e Falta de Treinamento dos funcionários |
| [P05] | Engenharia Social e a vulnerabilidade quanto aos princípios de Disponibilidade, Confidencialidade e Integridade |
| [P06] | Engenharia Social |
| [P07] | Engenharia Social |
| [P08] | Engenharia Social |

Quanto as respostas da QP1, as publicações [P02], [P03], [P04] e [P05] tiveram como principal ameaça a vulnerabilidade quanto aos princípios da segurança da informação: a disponibilidade, a confidencialidade e a integridade. A disponibilidade significa deixar disponível a informação sempre que necessário às pessoas autorizadas. A confidencialidade significa a garantia do segredo das informações, liberando-as apenas para pessoas autorizadas. A integridade é a garantia de que a informação não foi alterada indevidamente (CARVALHO e GALVÃO, 2015).

As organizações que não atentam aos princípios da segurança da informação correm mais riscos de sofrer ataques da Engenharia Social, pois a maioria dos ataques estão ligadas diretamente os fatores humanos (CARVALHO e GALVÃO, 2015; JUNIOR e BARCAROLLI, 2016). Isso foi bastante evidente nessa pesquisa, pois o indivíduo que pratica a Engenharia Social geralmente explora traços comportamentais do ser humano, como a persuasão, a vontade de ser útil, a busca por novas amizades e a propagação da responsabilidade (COELHO, RASMA e MORALES, 2013)

As vulnerabilidades dos princípios da segurança da informação podem facilitar outros tipos de ataques que não utilizam Engenharia Social, que geralmente são os ataques cibernéticos utilizando softwares sofisticados de ataque. Mas a Engenharia Social também pode usar softwares para ataques, embora sua principal característica seja a manipulação dos sentimentos humanos (SILVEIRA, REALAN e AMARAL, 2016), e talvez seja por este motivo dela ser identificada como principal ameaça em todas as publicações selecionadas.

- **Análise e Discussão da QP2**

Sobre a segunda questão "Quais as técnicas utilizadas pela engenharia social?", apresentadas na Tabela 5, há uma técnica predominante em todos os artigos: *Phishing*, que significa uma forma de enviar mensagens falsificadas através de correio eletrônico para pessoas que acabam entregando dados confidenciais, tais como número de cartão, documentos e senhas, por estas mensagens parecerem de organizações como bancos renomados, governos ou multinacionais (SILVA, 2012).

**Tabela 5 – Resultados da QP2 identificadas nas publicações selecionadas**

| ID | Técnicas Utilizadas pela Engenharia Social |
|---|---|
| [P01] | *Phishing*, Análise em sites de Rede Social e Análise do Lixo |
| [P02] | *Phishing* e Exploração do Fator Humano |
| [P03] | Exploração do Fator Humano |
| [P04] | *Phishing*, Exploração do Fator Humano e Abordagem Pessoal |
| [P05] | *Phishing e* Coleta de dados via Internet e Redes Sociais |
| [P06] | *Phishing* e Coleta de dados via Internet para realizar os ataques cibernéticos |
| [P07] | *Phishing* e Coleta de dados via Internet para realizar os ataques cibernéticos |
| [P08] | *Phishing* e Coleta de dados via Internet para realizar os ataques cibernéticos |

Através da técnica "Análise em sites de Rede Social" os engenheiros sociais podem conhecer melhor o perfil de suas vítimas, que podem ser, por exemplo, funcionários de uma empresa que ele deseja atacar (SILVA, 2012). Percebe-se que essa é uma técnica bastante relacionada com a coleta de dados via Internet presente das publicações [P05], [P06], [P07], e [P08], por utilizar a exploração da vulnerabilidade das pessoas para divulgarem seus dados sem desconfiar de ataques maliciosos.

É importante discutir sobre a técnica de "Análise do lixo", citada na [P01], pois essa é um dos primeiros passos para atacar uma organização, porque na maioria das vezes ninguém observa o que está sendo descartado e de que forma é realizado o descarte de papéis ou demais objetos da empresa. O que pouco sabem é que o lixo é uma das fontes mais ricas de um engenheiro social, pois podem conter nome de funcionários, telefones, e-mails, contatos de funcionários ou clientes, senhas e muitos outros dados suficientes para a realização de uma ação dos engenheiros sociais (SILVA, 2012).

Pode-se afirmar também que a exploração do fator humano é a principal vulnerabilidade nas organizações, pois o ser humano possui medo, confiança, curiosidade, instinto de querer ajudar, ingenuidade entre outros fatores. Para quem possui habilidades extraordinárias de persuasão, manipular sentimento torna-se uma tarefa fácil (JÚNIOR e BARCAROLI, 2016). Uma organização é feita de pessoas que podem cometer erros, e o grande problema do erro humano é que ele não pode ser completamente corrigido, apenas minimizado, e nem o treinamento mais rigoroso pode mudar isso (CARVALHO e GALVÃO, 2015).

## Considerações Finais

A segurança da informação ainda é bastante vulnerável nas empresas devido aos poucos investimentos, tanto em ferramentas quanto em treinamentos de funcionários. O objetivo desse trabalho foi mostrar as principal ameaça à segurança da informação nas organizações e reportar as técnicas mais utilizadas pela engenharia social.

Como resultado foi obtido que a Engenharia Social é a principal ameaça a segurança da informação devido a facilidade de veiculação da informação e a ingenuidade e confiança das pessoas. No que se refere às técnicas, podemos citar o *Phishing* como a mais utilizada, segundo as pesquisas selecionadas. Essa técnica estimula pessoas a fornecer dados pensando que serão disponibilizados a pessoas ou organizações de sua confiança, quando na verdade são fornecidos a engenheiros sociais que se aproveitam da ingenuidade das pessoas, pois sabem explorar com sutileza o fator humano.

Como trabalho futuro podemos sugerir pesquisas *in loco*, utilizando coleta de dados em empresas no interior do Amazonas e nas prefeituras dos municípios para saber se os ataques da Engenharia Social são recorrentes nesses lugares, quais as técnicas mais utilizadas para isso e quais os perfis das vítimas que sofreram esses ataques em cada organização. Pesquisas como estas podem servir de base para a criação de cartilhas de segurança e treinamento de pessoas.

## Referências

ALENCAR, G.; LIMA, M.; FIRMO, A. O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO. **Anais**, João Pessoa, 2013, p. 254-259.

BRAGA, P. **Técnicas de Engenharia Social.** Grupo de Resposta a Incidentes de Segurança. UFRJ. Rio de Janeiro, 2010

CARVALHO, C.; GALVÃO, A. Engenharia Social: Uma Análise de Ameaças e Cuidados aos Funcionários das Agências Bancárias de Santarém e Itaituba – Pará. **Revista de Publicação Acadêmica da Pós-Graduação do IESPES**, 2015.

COELHO, C.; RASMA, E.; MORALES, G. Engenharia Social: Uma Ameaça à Sociedade da Informação. **Revista Científica Perspectivas Online**, v. 3, n. 05, 2013

FILHO, G. **Hackers e Crackers na Internet: As Duas Faces da Moeda.** Eletrônica Temática. Local. v. 1, n. 01, jan. 2010. Disponível em: <http://www.insite.pro.br/2010/janeiro/hackers_crackers_internet.pdf> Acesso em 16 fev. 2017.

JUNIOR, J.; BARCAROLI, V. Engenharia Social e a Aleatoriedade na Escolha do Alvo. **Revista Tecnológica**, v. 5, n. 2, 2016.

KITCHENHAM, B.; CHARTERS, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. **Relatório Técnico Evidence-Based Software Engineering (EBSE)**, v. 2.3, 2007.

MACHADO, C.; CABRAL, L.; SANTOS, J.; MOTTA, G. Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. V SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO. **Anais,** 2009**,** Brasília, p. 97-108.

MARCIANO, J. **Segurança da Informação – Uma Abordagem Social**. 2006. 212 f. Tese (Doutorado em Ciência da Computação) – Departamento de Ciência da Computação, Universidade de Brasília, Distrito Federal. 2006.

MITNICK, K., SIMON, W. **A Arte de Invadir: As Verdadeiras Histórias por Trás das Ações de Hackers, Intrusos e Criminosos Eletrônicos**. São Paulo: Person, 2005.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATISSON, M. Systematic Mapping Studies in Software Engineering. In: PROCEEDINGS OF THE EVALUATION AND ASSESSMENT IN SOFTWARE ENGIREENING (EASE), Bari, Italy, 2008.

SILVA, A. Engenharia Social: O Fator Humano na Segurança da Informação. **Revista das Ciências Militares,** 2010.

SILVA, C. Engenharia Social: O Elo mais Frágil da Segurança nas Empresas. **Revista Eletrônica do Alto Vale do Itajaí**, 2012.

SILVEIRA, A.; REALAN, M.; AMARAL, E. Engenharia Social: Uma Análise sobre o Ataque de Phishing. CONGRESSO SUL BRASILEIRO DE COMPUTAÇÃO. **Anais**, 2016, v. 8.