ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO

Cristiano Farias Coelho
Mestrando em Engenharia de Produção pela UENF
coelho@uenf.br

Eline Tourinho Rasma
Licencianda em Química pela UENF
elinerasma@hotmail.com

Gudelia Morales
Doutora em Engenharia de Sistemas e Computação pela UFRJ
gudelia@uenf.br

Recebido: 22 de outubro de 2012. Revisado: 05 de março de 2013. Aceito: 06 de março de 2013.

Publicado online: 23 de março de 2013.

RESUMO

O artigo trata de uma revisão bibliográfica do tema Engenharia Social em virtude do avanço das Tecnologias da Informação e Comunicação (TIC's). Expõe a vulnerabilidade da Sociedade da Informação ante a facilidade de veiculação das informações provocada pela comunicação de redes digitais distribuídas. A metodologia faz consulta a trabalhos científicos já publicados na busca problematizar a questão no meio corporativo, que tem nas informações seu recurso vital, pois delas dependem uma gestão de operações eficaz. Assim, o artigo identifica regras e procedimentos com vistas à segurança da informação, de maneira a prevenir uma das formas mais comuns de fraudes, a Engenharia Social, que afeta o componente mais frágil do sistema, o usuário.

Palavras-chave: Tecnologia da informação e comunicação; Engenharia social; Segurança da informação.

ABSTRACT

This paper is a literature review about Social Engineering due to the Information and Communication Technologies (ICTs) advancement. It exposes the vulnerability of the Information Society at the ease of flow of information caused by distributed digital communication networks. The methodology consults scientific works already published to discuss the issue in the corporate environment, which has information on their vital resource, because the dependence on effective management of operations. Thus, this paper identifies rules and procedures with a view to information security in order to prevent one of the most common forms of fraud, Social Engineering, which affects the weakest component of the system, the user.

Keywords: Information and communication technologies; Social engineering; Information Security.

1. INTRODUÇÃO

O surgimento dos computadores e de sua interconexão em redes permitiu uma maior capacidade de processamento e de distribuição das informações. A Internet, importante ferramenta de tecnologia atualmente, é a rede mundial de computadores que propicia uma maior rapidez, eficiência e aumento na produção, manuseio e transmissão de dados (GANDINI; SALOMÃO; JACOB, 2002).

A sociedade se torna com o passar do tempo mais dependente dos computadores e das redes, devido aos benefícios oferecidos pela alta tecnologia que cresce em enorme escala. Devido a isso, segundo Marciano e Marques (2006), várias formas de ameaças, tanto físicas quanto virtuais, proliferam-se dentro deste universo de conteúdos, que comprometem seriamente a segurança das pessoas e das informações, bem como das transações que envolvem o complexo usuário-sistema-informação. Logo, revelou-se uma preocupação com a administração das informações trocadas entre usuários, em redes de computadores, tornando-se indispensável à adoção de procedimentos que visem à segurança das informações.

De acordo com Marciano e Marques (2006), a Tecnologia da Informação e Comunicação (TIC) é capaz de apresentar parte da solução a este problema, não sendo, contudo, capaz de resolvê-lo integralmente, ou até mesmo contribuir em agravar o problema, em alguns casos. Com isso é possível afirmar que, não existem sistemas totalmente seguros, porém através da segurança da informação, há meios de reduzir esses riscos.

Assim, baseado em trabalhos de investigação já publicados no meio científico, o presente artigo se propõe a apresentar uma revisão bibliográfica acerca da Engenharia Social, tema ainda pouco difundido apesar do avanço das Tecnologias da Informação e Comunicação (TIC's). O artigo busca contribuir também na identificação de regras e procedimentos com vistas à segurança da informação.

2. METODOLOGIA

O artigo desenvolveu um estudo de caráter qualitativo, e tem como objetivo uma pesquisa exploratória do tema Engenharia Social, dentro do novo contexto apresentado pelas Tecnologias da Informação e Comunicação (TIC's), através de um levantamento bibliográfico. Para tanto, inicia-se com uma visita à história da evolução da informação e seus registros, que possibilitariam formar mais tarde um conjunto de regras e procedimentos para garantir sua integridade e inviolabilidade.

A pesquisa bibliográfica é um dos principais recursos utilizados para o desenvolvimento deste trabalho, que, de acordo com Lakatos e Marconi (1991), procura explicar um problema a partir de referências teóricas publicadas em documentos. Ainda, de acordo com este autor, a pesquisa bibliográfica busca conhecer e analisar as contribuições culturais ou científicas existentes sobre um determinado assunto, tema ou problema. Abrange toda a bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico e meios de comunicação como rádio, gravações em fita magnética e audiovisual (filmes e televisão).

Assim sendo, este trabalho baseou-se no levantamento das idéias defendidas por autores da área relacionada à segurança na transmissão de informação. É feita uma abordagem das maneiras mais eficazes para o tratamento do problema, através da história da informação e sua classificação. Mostram-se alguns mecanismos de segurança da informação, os pontos que auxiliarão na melhoria desta e de como a engenharia social atua, e quais podem ser as formas de prevenção e treinamento, para se evitar tais ataques.

O artigo buscou problematizar a questão no meio corporativo, que tem nas informações seu recurso vital, pois delas dependem uma gestão de operações eficaz. Assim, o artigo identifica regras e procedimentos com vistas à segurança da informação, de maneira a prevenir uma das formas mais comuns de fraudes, a

Engenharia Social, que afeta o componente mais frágil do sistema, o usuário.

3. A HISTÓRIA DA INFORMAÇÃO E SUAS FORMAS DE REGISTRO

Há milhares de anos, desde o início da existência da humanidade, é possível perceber que sempre houve uma constante preocupação em gerar registros de conhecimentos que eram produzidos. E à medida que a sociedade evoluía, aumentava-se a preocupação com as informações geradas, consequentemente com a segurança das mesmas (GONÇALVES, 2005).

Os primeiros registros são de artes rupestres em 30.000 a.C., por homens pré-históricos, que ilustravam seus sonhos, símbolos como da vida e da morte, além de cenas do cotidiano, através de das representações pictóricas (ROCHA, 2008). Após vieram a escrita cuneiforme criada pelos sumérios em 3.500 a.C., produzida com o auxílio de objetos em formato de cunha e a escrita codificada, chamada de hieróglifo, formada por um conjunto de sinais pictográficos em 2.700 a.C., produzida pelas castas dominantes da civilização egípcia, visto a complexidade da informação e o seu valor (SIRUGI, 2008; PACIEVITCH, 2008).

Em 23 a.C. o correio romano utilizou como transporte oficial de informações, um serviço postal denominado Cursus Publicus, organizado por mensageiros a pé e a cavalo, dispostos em várias distâncias nas estradas de comunicação, à serviço unicamente dos órgãos do Estado (MEIRELLES, 1983).

Os materiais para gravar informações evoluíram incrivelmente, desde a invenção do papel em 105 d. C., atribuído a T'sai Lun, na China (ADAMS, 2012). À medida que a aumentou a necessidade de registrar informações, ocorreu também a necessidade de divulgá-las. Então, Johannes Gutenberg, em 1450, inventou a prensa móvel, o que provocou a disponibilização da informação às massas, fomentando uma revolução na produção de livros, assim como o rápido desenvolvimento das ciências, artes e religião, através da transmissão de textos (BELLIS, 2007).

Com este desenvolvimento veio a evolução das formas de registro da informação através da tecnologia, que em 1876 registrou a invenção do telefone, por Alexander Graham Bell. Em 1946 a contribuição se deu com o ENIAC, primeiro computador eletrônico utilizado na Segunda Guerra Mundial, para auxiliar o exército norte-americano a fazer cálculos de balística (BARROS, 2008; PRIMEIRO..., 2006).

Desde então, devido ao progresso tecnológico, os computadores deixaram de ser restritos aos militares e às empresas, ficando ao alcance do usuário doméstico. A partir deste desenvolvimento, os sistemas operacionais foram melhorados e o lançamento do Windows 95 foi considerado como a era dos fax/modems, do e-mail, das notícias online, dos jogos multimídia e dos programas educacionais (PISA, 2012).

A evolução da tecnologia veio acompanhada das diversas formas de ameaças tanto virtuais quanto físicas, comprometendo a segurança das informações e dos usuários que as usufruem. Essa ocasião de insegurança na utilização de meios virtuais para informação se deu com o primeiro vírus lançado no sistema, através de disquetes, criado por um estudante de 15 anos, em 1982, contudo, o vírus não oferecia nenhum risco ao sistema (ROHR, 2008).

Em 1984, criou-se a ISSA – Information Systems Security Association, a primeira associação internacional para profissionais de segurança de sistemas (RICHARDS, 2001). Em 1989, a IBM forneceu o primeiro antivírus específico comercial (HISTÓRIA..., 2008).

Desde então, a segurança tem sido incorporada ao cotidiano, pois a criatividade dos criminosos, que aproveitam a ingenuidade das pessoas, encontra um campo fértil para roubo e furtos virtuais, uma vez que também não há sistemas totalmente seguros. Porém, com a ajuda também da tecnologia, são criados meios eficazes de reduzir os riscos relacionados à segurança da informação (SANTOS, 2008).

4. CLASSIFICAÇÃO DA INFORMAÇÃO

Define-se dado como qualquer elemento identificado na sua forma bruta, que por si só não conduz a uma compreensão de um determinado fato ou tema. Ao passo que por informação, entende-se como um conjunto de dados articulados entre si, que depois de trabalhados ou processados, produzem um determinado sentido ou significado sobre um assunto. A palavra informação vem do latim *informationem*, que significa "delinear", "conceber uma idéia", ou seja, dar forma ou moldar na mente. Segundo Rezende e Abreu (2000), informação é o dado com uma interpretação lógica ou natural agregada pelo usuário. A informação é um bem ou ativo que, como qualquer outro é importante para os negócios, que tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido, conforme recomenda a Norma Brasileira NBR ISO/IEC 17799 de 2003.

Conforme afirmam Laureano e Moraes (2005), nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, uma determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda, será menor que o custo de não dispor dela adequadamente. Segundo os autores, a informação pode ser classificada de acordo com o seu nível de sigilo, priorizando o emprego dos recursos a ela estabelecidos, ou seja, pode ser informação:

- Pública: não oferece potencial de risco a um sistema, pois sua integridade não é vital, podendo a informação ser divulgada ao público externo, de tal forma que incentivará a competição do negócio e/ou imagem;
- Corporativa ou Interna: somente os usuários internos de um sistema terão acesso à informação, tendo como conseqüência não tão séria, se por acaso houver um acesso não autorizado. Apesar, de sua integridade não ser vital ao sistema, ela é sim, muito importante;
- Confidencial: neste caso, o cuidado com a informação é fundamental, pois garante a um sistema a obtenção de vantagens competitivas, ou seja, divulgação ou perda desta pode levar ao desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo;
- Secreta: se expostas, podem ocasionar danos graves ou irrecuperáveis de nível político e/ou estratégico. Por isso a segurança desse tipo de informação é vital para uma companhia.

Caso as informações não estejam rotuladas definitivamente, estas devem ser classificadas como corporativas, até que sejam regularizadas. Como apontam Laureano e Moraes (2005) ao notar que, algumas informações são centrais para a organização, e sua divulgação parcial ou total pode acarretar repercussões cuja complexidade pode ser pouco ou nada administrável pela organização. E recomendam cuidado com a integridade, a precisão, a atualidade, a interpretação e o valor geral da informação, por isso é indispensável o uso de sistemas de segurança para a gestão da informação e os dados operacionais.

A informação é um ativo importante das organizações, senão o mais importante, e com isso torna-se indispensável à proteção adequada para todo o seu ciclo de vida: começando na criação, manipulação, armazenamento, transporte e descarte. As fases do ciclo se distribuem da seguinte forma, de acordo com Oliveira (2011):

- Manipulação: este ato reúne os processos de criação, alteração e processamento da informação. Nesta fase, ocorre a maior parte dos lapsos em relação à segurança, pois há maior interação entre a informação e as entidades que a utilizam;
- Armazenamento: refere-se ao armazenamento e arquivamento da informação em meios digitais, magnéticos ou qualquer outro que a suporte. Nesta fase, deve-se preservar os pilares da segurança da informação, a tríade *Confidentiality, Integrity and Availability* – CIA (do inglês Confidencialidade, Integridade e Disponibilidade), representada pela Figura 1, de acordo com a necessidade de cada informação, pois está sujeita a riscos naturais de alteração. A fase de arquivamento compreende-se como

um processo de guarda das informações que não estão mais em produção, ou seja, se transformam em arquivos mortos para a entidade;

- Transporte: refere-se aos atos de movimentação e transferência da informação, entre processos, mídias ou entidades internas ou externas. No transporte se consideram todos os tipos de comunicação como cartas, e-mails, pastas de arquivos, *notebooks* e *pen drives*, telefones e transmissões eletrônicas via rede, inclusive, o diálogo falado, pois ao falar, a informação é transportada pelo ambiente, ou seja, pelo ar, e assim pode-se deixar vazar informações valiosas;
- Descarte: refere-se às ações de descarte e destruição das informações no meio em que se encontram. Os documentos que não tiverem mais utilidades devem ser triturados, inclusive os que irão para a reciclagem, e os documentos eletrônicos devem ser transferidos para uma mídia transportável, chamadas de firewalls. Tudo isso, é cabível para uma maior segurança das informações ali contidas. Cada meio requer um tipo de cuidado especial em relação à exclusão, para que as informações estejam sempre protegidas, mesmo sendo descartadas, como inservíveis.

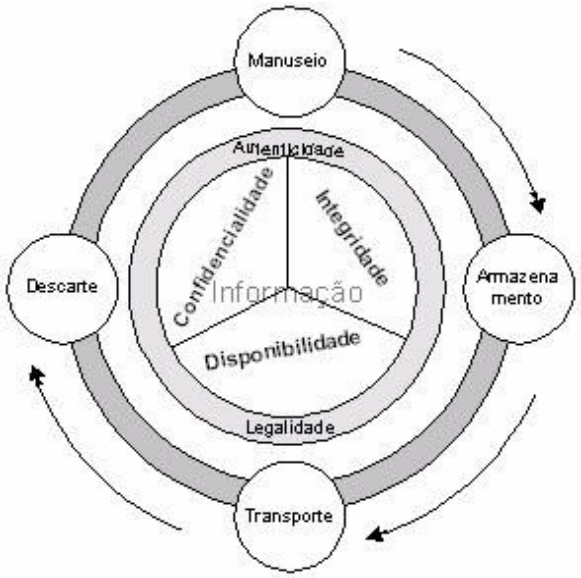

Figura 1: Fases do Ciclo de Vida da Informação (LAUREANO, 2005)

5. SEGURANÇA DA INFORMAÇÃO

De acordo com Silva e Stein (2007), hoje a Segurança da Informação se tornou um problema importante da sociedade moderna. Desde grandes empresas a indivíduos comuns, todos têm o direito de esperar que seus dados privados sejam mantidos intactos e disponibilizados apenas a pessoas autorizadas.

Segundo Santos (2011), a principal ameaça para qualquer segurança é sem dúvida o ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema. A segurança da informação, cada vez mais, é considerada uma questão de comportamento para a que deve formar-se uma cultura. Por exemplo, muito cedo se aprende a não falar com estranhos, a não deixar a porta de casa aberta, entre outras coisas, pois a integridade, tanto física quanto moral, depende dessas atitudes, e essa necessidade de proteção se mantém ao longo da vida.

Esse comportamento defensivo é considerado uma questão de sobrevivência neste momento atual conhecido também como Era Digital. O grande desafio da segurança da informação, no presente, é desenvolver a cultura sobre os riscos deste novo mundo, cada vez mais real-virtual, sendo necessário realizar trabalhos de conscientização e treinamento entre os usuários e profissionais de segurança, no sentido de incorporar o hábito da segurança na rotina dos indivíduos.

Com o avanço da tecnologia, as empresas que querem se manter no mercado, cada vez mais competitivo e globalizado, são obrigadas a realizar investimentos maciços em Tecnologia da Informação (TI). Ao fazer uso de ferramentas computacionais, para melhor manipular o grande volume de informações em circulação tanto ao nível local, onde eles atuem, quanto no mundial. Devido a freqüente mudança na forma como os sistemas permitem a troca de informação entre os setores corporativos, ainda é grande a dificuldade dos softwares, empregados para esse fim, em oferecer uma forma de criptografar as mensagens, e assim, toda a informação trafega livremente pela rede interna da empresa.

De acordo com Ferreira et al. (2010), a simples instalação de um analisador de pacotes, conhecido como *sniffer*, pode interceptar as conversas em formato de texto. Percebe-se que não é necessário ser um perito em informática para conseguir informações privilegiadas, porém o simples uso de criptografia poderia facilmente impedir esse acesso não autorizado.

Para isso surgiram as normas que ajudam a formular as políticas de segurança da informação, as políticas de utilização de ativos, padronização de procedimentos, aplicação de mecanismos de segurança, dentre outros (SIEWERT, 2008).

6. RESULTADOS E DISCUSSÃO

Engenharia Social é o termo utilizado para definir a área que estuda as técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma organização, através das pessoas, funcionários e colaboradores de uma corporação ou de uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança. (EIRAS, 2004)

Para Hadnagy e Maxwell (2009), a engenharia social no contexto da segurança no uso de tecnologias de informação e comunicação se refere às ações praticadas para obter e quebrar o valor da informação. Também para obter dados importantes e sigiloso de organizações e/ou sistemas computacionais, por meio da exploração da confiança das pessoas.

Levando-se em conta o significado de cada uma das palavras, conforme pesquisa realizada por Peixoto (2004), o termo Engenharia Social não parece ter a conotação maléfica que carrega consigo:

- Engenharia: Arte de aplicar conhecimentos científicos, empíricos e certas habilitações específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas;
- Social: Da sociedade, ou relativo a ela. Sociável. Que interessa à sociedade.

Porém, a engenharia social não é baseada em ciência natural, mas sim nas ciências humanas e sociais, tais como a filosofia, psicologia, economia, próximas com teorias básicas dos seres humanos e a sociedade (WHAT IS..., 2006).

Assim, a junção das duas palavras anteriormente definidas traz um significado bem diferente da ideia de harmonia e equilíbrio que expressam quando utilizadas separadamente:

- Engenharia Social: designa a arte de manipular pessoas a fim de contornar dispositivos de segurança. É baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores de um sistema (ENGENHARIA..., 2009).

Engenharia Social no contexto das Ciências Políticas consiste em técnicas e artes dirigidas a manipulação das pessoas para conseguir que elas realizem atos que normalmente não fariam, em grande escala, ou divulguem voluntariamente informações pessoais ou da empresa onde prestam serviço; explorando a vulnerabilidade humana (HADNAGY; MAXWELL, 2009).

O ataque às Torres Gêmeas (Nova Iorque, 2001), foi um marco para a adoção definitiva de medidas

enérgicas de proteção. O terrorismo e a criminalidade transformaram, desde então, o conceito de segurança, tanto da população quanto da informação. A ideia defendida por Aposkitis (2009), por exemplo, é que a atual situação social no mundo seja um produto de técnicas de engenharia social, que operam no fundo das questões políticas, assistência social, economia, informação, cultura, indústria, entretenimento e marketing.

O mesmo autor acredita que o objetivo dessa técnica seja manipular cidadãos aproveitando a passividade deles destruindo as tradições de nações, sociedades e sistemas religiosos a fim de aumentar os lucros das empresas multinacionais. Segundo esta corrente, a desconstrução social seria aplicada no mundo todo, através da prática de guerras e terrorismos. Todas essas ações apresentadas resultariam do projeto de uma elite internacional, segundo um modelo capitalista de mercado, que tornam as pessoas totalmente entregues e incapazes de defender suas conquistas sociais, símbolos nacionais e liberdades civis adquiridas após larga luta (APOSKITIS, 2009).

Geralmente o engenheiro social é um tipo de pessoa agradável, educada, simpática e carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente. Até, mesmo, pessoas sem conhecimento antecipado desta denominação, já cometeram algum ato de engenharia social involuntariamente (PEIXOTO, 2004).

Existem várias formas de ataques, sempre explorando a fragilidade e a ingenuidade das pessoas. Estes ataques podem ter dois enfoques diferentes: o físico, como local de trabalho, lixo, telefones; e o psicológico, como persuasão, criando confiança, ou simplesmente, sendo gentil.

Silva Filho (2004) mostra os traços comportamentais, que tornam o ser humano susceptível a ataques:

- Persuasão – Compreende quase uma arte a capacidade de induzir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação;
- Vontade de ser útil – O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário;
- Busca por novas amizades – O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações;
- Propagação de responsabilidade – Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

Com a evolução do comércio eletrônico e sistemas rotineiros automatizados, a forma mais comum de ataque da engenharia social é *on line*, e com isso aumentou a preocupação quanto à privacidade que, segundo o autor Bellavista (1991), refere-se ao direito que um indivíduo possui de controlar o uso que outros fazem das informações que digam respeito a ele.

Neste sentido, para garantir a qualidade técnica e um maior controle na disseminação dos serviços ofertados pela Internet, houve a necessidade da intervenção do Estado, foi criado em maio de 1995 o Comitê Gestor da Internet, um esforço conjunto do Ministério das Comunicações e do Ministério da Ciência, Tecnologia e Inovação (CGI.br, 2010).

Aparentemente na contramão deste raciocínio, em 2011 foi criada a Lei nº 12.527, conhecida como "Lei de Acesso à Informação", cujo princípio é que as informações referentes à atividade do Estado são públicas, salvo exceções expressas na legislação, e adota inclusive os recursos da TI a fim de facilitar e agilizar o acesso por qualquer pessoa. Os objetivos da norma são fomentar o desenvolvimento de uma cultura de transparência e o controle social na administração pública (BRASÍLIA, 2012).

Porém, a mesma Lei em questão prevê como exceções de divulgação de informações, aquelas de ordem pessoal, relativas à intimidade, vida privada, honra e imagem. De acordo com Ferreira (2008), a Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. É um conjunto de mecanismos que deve ser

adequado a um determinado ambiente ou infra-estrutura.

A segurança da informação considera os seguintes elementos, como principais pilares, para orientar a análise, o planejamento e a implementação de tal, a chamada tríade CIA, de acordo com Siewert (2008):

- Confidencialidade: significa garantir o segredo das informações, liberando acesso somente às pessoas autorizadas; a perda deste atributo ocorre quando pessoas não autorizadas obtêm acesso às informações confidenciais;
- Integridade: significa garantir que a informação não foi alterada indevidamente, ou seja, devem-se manter as características originais impostas pelo proprietário da informação, mantendo o seu ciclo de vida (nascimento, manutenção e destruição);
- Disponibilidade: significa garantir a disponibilidade da informação, sempre que necessário às pessoas autorizadas.

Quando é usado o processo criptográfico de proteção de informações, outros atributos importantes são a Irretratabilidade (o emissor não pode negar a veracidade da mensagem ou assinaturas) e a Autenticidade (o receptor deve poder verificar que a assinatura é feita pelo emissor).

O nível de segurança desejado pode ser alcançado através de políticas de segurança da organização. Segundo Böger e Bodemüller (2007) elas formam um conjunto de regras que especificam como um sistema deve prover os seus serviços, limitar as operações dos usuários e determinar como as informações e os recursos devem ser administrados, protegidos e distribuídos no interior de um sistema específico. Os principais mecanismos de segurança são divididos em:

- Controles administrativos: que são as políticas de segurança;
- Controles físicos: que são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura, garantindo a existência da informação, que a suporta. Como portas, paredes, trancas, blindagem, guardas;
- Controles lógicos: que são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico. Exemplos disto são os mecanismos de criptografias, assinatura digital, mecanismos de certificação, controle de acesso, entre outros.

Para colocar em prática tais mecanismos de segurança, deve-se levar em conta, principalmente, os riscos associados à carência deles à segurança, os benefícios esperados e os custos da implantação dos mesmos.

7. CONCLUSÕES

À medida que a sociedade moderna se torna cada vez mais dependente da informação, a engenharia social tende a crescer e constituir-se numa das principais ameaças aos sistemas de segurança das (grandes) organizações (SILVA FILHO, 2004).

Isso se justifica no fato de que o sucesso ou fracasso delas depende da tomada de decisões, que as instituições se baseiam em dados e informações. Assim, espera-se que estes sejam de qualidade e tenham sua integridade garantida. De acordo com Mitnick (2001), uma empresa pode gastar fortunas com aquisição de tecnologias e serviços, mas a sua infraestrutura de rede pode ainda ser vulnerável a antigos métodos de manipulação. Isso é possível porque a engenharia social explora o elo mais fraco do sistema de segurança de informação, o ser humano (EIRAS, 2004).

Entretanto, existem várias ferramentas para minimizar os problemas decorrentes pela engenharia social causados por vulnerabilidades, através de mecanismos de segurança como criptografia, assinatura digital, antivírus, controle de acesso (senhas, firewalls, sistemas biométricos e *smartcards*), políticas de segurança, dentre outros.

Para minimizar as perdas referentes aos ataques da engenharia social, deve-se: programar políticas de segurança nas organizações e sua ampla divulgação; promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social; realizar a classificação e armazenamento da informação conforme o seu nível; executar a implementação e monitoramento dos mecanismos de segurança; não manusear informações corporativas fora da empresa e nem fornecer informações pessoais ou secretas; tomar cuidados especiais com o lixo eletrônico, assim como em qualquer outro meio, através de regras de descarte.

Segundo Santos (2011), a principal ameaça para qualquer segurança é o próprio ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema. Assim, para se proteger dos oportunismos da engenharia social, a sociedade da informação deve criar uma cultura que incentive um comportamento humano consciente no domínio das informações, a fim de evitar riscos de perdas, pessoais ou corporativas.

8. REFERÊNCIAS

ADAMS, B. G. Diversos textos sobre a invenção e história do papel e também diversas formas práticas de fabricação de papel reciclado encontrados na internet. Disponível em: < http://www.apoema.com.br/pape1.htm> Acesso em 14 jul. de 2012.

APOSKITIS, L. Social Engineering: The absolute war in full development. Journal of Hellenic Nexus, dez. 2009. Disponível em: <http://thegreek.hubpages.com/hub/Social-Engineering-The-absolute-war >. Acesso em: 05 set. 2012.

BARROS, J. Dia do Telefone. 2008. Disponível em: <http://www.brasilescola.com/datacomemorativas/dia-telefone.htm>. Acesso em: 21 jul. 2012.

BELLAVISTA, A. Quale legge sulle banche datti? Rivista Critica del Diritto Privato. v. 9, n. 3, set. 1991.

BELLIS, M. Johannes Gutenberg and the Printing Press. 2007. Disponível em: < http://inventors.about.com/od/gstartinventors/a/Gutenberg.htm>. Acesso em: 15 jul. 2012.

BÖGER, D. S.; BODEMÜLLER JUNIOR, R. Segurança da Informação. 2007. Disponível em: < http://www.das.ufsc.br/~dsboger/aula/07_1/ine5329-administracao_em_processamento_de_dados/transparencias_seguranca.pdf>. Acesso em 18 jul. de 2012.

BRASÍLIA. Câmara dos Deputados. Lei de acesso à informação: cartilha de orientação ao cidadão. 2012. Disponível em: <http://www2.camara.gov.br/transparencia/lei-de-acesso-a-informacao/cartilha-do-cidadao-lei-de-acesso-a-informacao>. Acesso em: 17 set. 2012.

CGI.br - Comitê Gestor da Internet no Brasil. Sobre o CGI.br. 2010. Disponível em:<http://www.cgi.br/sobre-cg/index.htm>. Acesso em: 25 jul. 2012.

E O PC ganha força no mercado mundial. A Tribuna. Santos. 12 abr. 2000. Disponível em: < http://www.novomilenio.inf.br/ano97/97hist04.htm>. Acesso em: 21 jul. 2012.

EIRAS, M. C. Engenharia Social e Estelionato Eletrônico. 2004. 40f. Monografia (Conclusão de Curso – lato sensu). IBPINET – The internet school e Uni-Rio, Graduação em Segurança da Informação na Internet, Rio de Janeiro.

ENGENHARIA Social. 2009. Disponível em: <http://pt.kioskea.net/contents/attaques/ingenierie-sociale.php3>. Acesso em: 22 jul. 2012.

FERREIRA, M. O que vem a ser segurança da informação? 2008. Disponível em: <

http://www.apinfo.com/artigo81.htm>. Acesso em: 15 jul. 2012.

FERREIRA M.; ALEXANDRINO, O.; PELIN, R.; JARDIM, W. Engenharia Social, a ação humana na prática ilegal de acesso à Informação. 2010. Disponível em:<http://fbvmanagersheet.googlecode.com/svn/trunk/ManagerSheet/ManagerSheet/Ambiente/Infraestrutura/Engenharia_Social_Paper.pdf>. Acesso em: 12 set. 2012.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. A segurança dos documentos digitais. Revista Jurídica: Órgão Nacional de Doutrina, Jurisprudência, Legislação e Crítica Judiciária, Porto Alegre, Ano 53, v. 50, n. 295, p. 59-71, mai. 2002.

GONÇALVES, L. R. O. Um modelo para verificação, homologação e certificação de aderência a norma nacional de segurança da informação – NBR-ISSO / IEC- 17799. 2005. 189f. Tese (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, COPPE – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Rio de Janeiro.

HADNAGY C.; MAXWELL, E. Social Engineering Defined. Social engineering framework. 2009. Disponível em: < http://www.social-engineer.org/framework/Social_Engineering_Defined >. Acesso em: 05 set. 2012.

HEITLINGER, P. Tipografia: origens, formas e uso das letras. Lisboa, 2006. Disponível em: < http://tipografos.net/glossario/manuscrito.html>. Acesso em: 13 jul. 2012.

HISTÓRIA: A Evolução do Vírus e Antivírus de Computador. 2008. Disponível em: < http://vomicae.net/programas/historia-a-evolucao-do-virus-e-antivirus-de-computador/>. Acesso em: 22 jul. 2012.

LAKATOS, E. M.; MARCONI, M. A. Fundamentos de metodologia científica. 3. ed. São Paulo: Atlas, 1991.

LAUREANO, M. A. P. Gestão de Segurança da Informação. 2005. Disponível em: < http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 21 jul.2012.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia, Paraná, v. 8, n. 3, p. 38-44, jan./mar. 2005.

MARCIANO, J. L.; MARQUES, M. L. O Enfoque Social da Segurança da Informação. Revista Ciência da Informação, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006.

MEIRELLES, A. T. História do comércio internacional. 1983. Disponível em: < http://www.consciencia.org/historia-do-servico-postal>. Acesso em: 20 jul. 2012.

MITNICK, K. My first RSA Conference. 2001. Disponível em: <http://www.securityfocus.com/news/199> Acesso em: 6 set. 2012.

OLIVEIRA, S. Ciclo de vida da Informação – Gestão da Segurança da informação. 2011. Disponível em: < http://pt.scribd.com/doc/52566307/42/Ciclo-de-vida-da-informacao>. Acesso em 20 jul. 2012.

PACIEVITCH, T. Hieroglifos. 2008. Disponível em: < http://www.infoescola.com/civilizacao-egipcia/hieroglifos/> Acesso em: 14 jul. 2012.

PEIXOTO, M. C. P. Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações. 2004. 164f. Monografia (Conclusão de Curso). Centro Universitário do Triângulo, Pró- Reitoria de Ensino de Graduação de Ciência da Computação, Uberlândia.

PISA, P. A evolução do Windows. 2012. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2012/05/a-evolucao-do-windows.html>. Acesso em: 22 jul.

2012.

PRIMEIRO computador do mundo completa 60 anos. 2006. Disponível em: < http://tecnologia.terra.com.br/noticias/0,,OI892512-EI12882,00-primeiro+computador+do+mundo+completa+anos.html>. Acesso em: 21 jul. 2012.

REZENDE, D. A.; ABREU, A. F. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. São Paulo: Atlas, 2000.

RICHARDS, K. L. About ISSA. Information Systems Security Association. 2001. Disponível em: < http://www.issa.org/?page=AboutISSA>. Acesso em: 22 jul. 2012.

ROCHA, G. L. Pintura Rupestre. 2008. Disponível em: < http://www.jornallivre.com.br/77970/pintura-rupestre.html> Acesso em: 14 jul. 2012.

ROHR, A. Conheça as diferenças entre vírus, backdoors e spywares. 2008. Disponível em: < http://g1.globo.com/Noticias/Tecnologia/0,,MUL856176-6174,00-CONHECA+AS+DIFERENCAS+ENTRE+VIRUS+BACKDOORS+E+SPYWARES.html>. Acesso em: 22 jul. 2012.

ROSA, A. F. A. Engenharia Social – Explorando o elo mais fraco. 2004. 8f. (Pós- Graduação – lato sensu) Faculdade Tecnologia SENAI Florianópolis, Florianópolis. Disponível em: <http://securityone.com.br/artigos/resenha_engenharia_social.pdf>. Acesso em: 21 jul. 2012.

SANTOS, A. H. G. A história da segurança da informação. 2008. Disponível em: <http://www.slideshare.net/andrehor/a-histria-da-segurana-da-informao-presentation-902879>. Acesso em: 22. jul. 2012.

SANTOS, L. A. F. dos. Segurança da informação. 2011. Disponível em: < http://www.slideshare.net/luiz_arthur/seguranca-da-informao-introduo>. Acesso em 15 jul. 2012.

SIEWERT, V. C. A Constante Evolução Da Segurança Da Informação. 2008. Disponível em: < http://artigocientifico.uol.com.br/uploads/artc_1202929819_49.pdf >. Acesso em: 13 jul. 2012.

SILVA, D. R. P. da; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. Ciência e Cognição- Revista Científica. Rio de Janeiro. v. 10. n. p. 46-53. mar. 2007. Disponível em: < http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410>. Acesso em: 20 jul. 2012.

SILVA FILHO, A. M. Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações. Revista Espaço Acadêmico. Ano 4, n. 43, dez./2004. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm>. Acesso em: 22 jul. 2012.

SIRUGI, F. Escrita Cuneiforme. 2008. Disponível em: < http://www.infoescola.com/civilizacoes-antigas/escrita-cuneiforme/>. Acesso em: 14 jul. 2012.

WHAT is Social Engineering. Departament of social engineering Tokyo Institute of Technology. 2006. Disponível em: <http://www.soc.titech.ac.jp/information_En/whatissoc.html#pagetop >. Acesso em: 05 set. 2012.