A ENGENHARIA SOCIAL E OS PROFISSIONAIS DA INFORMAÇÃO DE ARQUIVOS EMPRESARIAIS

Tiago Braga da Silva
tiagobragadasilva@gmail.com
Departamento de Ciências da Informação
Universidade Federal do Espírito Santo

Attilio Provedel*
attilio@terra.com.br
Departamento de Ciências da Informação
Universidade Federal do Espírito Santo

RESUMO

O presente trabalho destaca a informação como produto, relacionando a definição de dado, informação, conhecimento e inteligência, para o seu uso como vantagem competitiva. Aborda a Sociedade da Informação, apontando características da informação valiosa e como a informação ocupa lugar de destaque nas organizações. Apresenta os princípios da Segurança da Informação, discutindo a Engenharia Social e caracterizando as formas de ataque do engenheiro social com enfoque nas unidades de informações arquivísticas. No âmbito de uma política de segurança da informação, propõe a educação e a formação dos profissionais da informação como uma das armas mais eficazes no combate às ações do engenheiro social e na prevenção de acesso indevido às informações arquivísticas empresariais.

PALAVRAS-CHAVE

Segurança da Informação. Engenharia Social. Profissionais da informação. Arquivos Empresariais.

1. INTRODUÇÃO

O tema abordado neste trabalho traz uma discussão para a comunidade dos profissionais arquivistas sobre a segurança das informações geridas pelas unidades de informações empresariais.

* Autor para contato.

Com o avanço tecnológico – especificamente das Tecnologias da Informação e da Comunicação (TICs) –, a informação se torna cada vez mais presente em todas as atividades humanas, como afirma Lopes (2000):

> O trabalhador desde final do século é urbano e, muitas vezes, desenvolve atividades vinculadas à informação. Isto não o tornou mais rico e nem, necessariamente, mais especializado. Mas vem modificando completamente, a sua inserção no mercado de trabalho, quando existente. Neste aspecto, o caixa do supermercado e o analista de sistemas de uma grande empresa se parecem. Ambos lidam com a informação.

Vivemos na Sociedade da Informação caracterizada, segundo Takahashi (2002) por "[...] uma nova era em que a informação flui a velocidades e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais". Tal constatação é corroborada por Bergmann (2004) quando essa autora afirma que a informação "Trata-se de um fenômeno global, com elevado potencial transformador das atividades sociais, políticas e econômicas, capazes de promover a integração entre pessoas, programas e projetos em diversos níveis. Assim, fica evidenciada cada vez mais a necessidade incondicional do uso correto e preciso da informação em virtude da mesma ser vista pelas organizações, públicas ou privadas como a principal responsável pelo funcionamento da engrenagem da administração de tais organizações.

Com a informação atingindo tal valor, os ataques à mesma se intensificaram. Atualmente a informação empresarial é alvo de freqüentes ataques, que são cada vez mais profissionais e elaborados, e ocorrem de diferentes maneiras. As instituições, por sua vez, vêm investindo altos valores em segurança da informação, no entanto, costuma-se investir muito em tecnologias e acabam esquecendo de outro recurso tão importante quanto à informação, a saber, os funcionários, que são os pilares de qualquer política de segurança da informação.

Neste cenário, de uma forma geral, buscou-se com uma revisão de literatura a discussão sobre as políticas de segurança da informação em ambientes empresarias, com o objetivo específico de abordar o ataque do engenheiro social em Unidades de Informação Arquivística (UIAs) e a importância da educação dos profissionais da informação que atuam em UIAs.

A Engenharia Social trata de um conjunto de ações que visam adquirir informações sigilosas de maneira fraudulenta, sem o uso da força bruta, usando apenas a indução capciosa

ao engano. Segundo Mitnick e Simon (2003), a Engenharia Social compara-se à arte teatral, que faz com que as pessoas façam coisas que normalmente não fariam para um estranho. E é dessa forma que o engenheiro social, quem pratica o ataque de Engenharia Social, obtém informações empresariais sigilosas.

O artigo foi estruturado da seguinte forma. A seção 2 aborda a informação como produto e seu lugar neste novo cenário econômico no mundo empresarial. Na seção 3, os princípios da Segurança da Informação são apresentados. Em seguida, a seção 4 conceitua a Engenharia Social e a seção 5 caracteriza as formas de agir do engenheiro social principalmente junto às unidades de informação arquivística. As considerações finais propõem, no âmbito de uma política de segurança da informação – seção 6 – a educação e a formação dos profissionais da informação como uma das armas mais eficazes no combate às ações do engenheiro social e na prevenção de acesso indevido às informações arquivísticas empresariais.

2. O POTENCIAL COMPETITIVO DA INFORMAÇÃO

Cruz (2002) hierarquiza a informação nos seguintes níveis: dado, informação, conhecimento e inteligência. Oliveira (1997), por sua vez, define dado como "[...] qualquer elemento identificador em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação" e "[...] Informação é o dado trabalhado que permite [...] tomar decisões".

Segundo Stair e Reynolds (1999), dados consistem em fatos não trabalhados e informação é uma coleção de fatos organizados de modo que adquirem um valor além do valor dos próprios fatos.

Ambas as definições tratam o dado como algo que antecede a informação, logo toda informação tem como antecedente o dado bruto, mas não significa que todo dado é informação. Como verificado, o dado só é informação se trabalhado, se contextualizado, se for agregado valor.

O dado precisa ser bem trabalhado, para constituir uma informação e para trazer resultados positivos a quem dela necessitar. A informação, por outro lado, gera o conhecimento, que, segundo Stair e Reynolds (1999), representa a percepção e a compreensão de um conjunto de informações e de como estas informações podem ser úteis para uma tarefa específica. Por sua vez, Araújo (2005) define conhecimento como sendo "(...) a informação valiosa da mente humana. Inclui reflexão, síntese e contexto. De difícil estruturação, difícil captura em máquinas, freqüentemente tácito e de difícil transferência".

O conhecimento é algo pessoal, intransferível, que cada indivíduo com sua cultura e seus valores diferenciados constituem ao longo de sua existência. Na hierarquia da informação abordada por Cruz (2002), o conhecimento não é o ponto máximo dessa hierarquização; tem-se a inteligência no cume da hierarquia, que este autor define como sendo o conhecimento depurado e, portanto, útil à tomada de decisão.

A obtenção da inteligência é, no entanto, o grande desafio para as empresas e pessoas que recebem informações. A articulação dos dados e das informações para se tornarem inteligência apresenta-se como um grande paradigma para a Sociedade da Informação.

As UIAs são responsáveis pela gestão orgânica da informação de instituições públicas ou privadas, ou seja, informações geradas e recebidas em diferentes suportes físicos durante a realização das atividades administrativas que, em suma, consiste no tratamento técnico da informação para melhor utilização nas tomadas de decisões. A Lei n°8.159/1991, em seu parágrafo 3°, considera a gestão de documentos como "(...) o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para a guarda permanente". Assim sendo, a gestão feita pelas UIAs tem três fases básicas: produção, utilização e destinação.

Uma empresa, para sobreviver e prosperar num mercado competitivo, terá que estar baseada na informação, na qualidade que ela contenha, nas implicações que ela imponha (DRUKER apud TONINI, 2006). A informação atingiu um patamar de importância não como simples resultado das atividades administrativas, mas como produto de relevância para o mercado.

Para Latres e Albagli (1999) "a informação e o conhecimento passaram a desempenhar um novo e estratégico papel, (...) assumindo um valor imensurável na tomada de decisões". Jardim (1999), quando se refere à economia da informação, trata do reconhecimento da informação como um recurso estratégico.

Segundo Stair e Reynolds (1999), se a informação não for precisa ou completa, decisões ruins podem ser tomadas. Segundo os mesmos autores a informação para ser valiosa tem que possuir as características expostas a seguir:

> Precisa: A informação precisa não contém erro. Em alguns casos, a informação imprecisa é gerada porque dados imprecisos são alimentados no processo de transformação.
> Completa: A informação completa contém todos os dados importantes. Por exemplo, um relatório de investimento que não inclua todos os custos importantes não é completo.

Econômica: A informação também deve ser relativamente econômica para ser viabilizada. Os tomadores de decisão sempre precisam equilibrar o valor da informação com o custo de produzi-la.

Flexível: A informação flexível pode ser usada para uma variedade de propósito. Por exemplo, a informação sobre estoque disponível para uma peça em particular pode ser útil para o vendedor num fechamento de venda, para o gerente de produção, que determina a necessidade ou não de mais estoque, e para o executivo financeiro, que especifica o valor total que a empresa investiu em estoque.

Confiável: A informação confiável pode ser dependente de algum outro fator. Em muitos casos, a confiabilidade da informação depende do método de coleta dos dados. Em outros exemplos, a confiabilidade depende da fonte da informação. Um rumor, sem fonte conhecida, sobre a elevação de preço do petróleo pode não ser confiável.

Relevante: A informação relevante é essencial para a tomada de decisão. A queda de preço da madeira pode não ser relevante para um fabricante de chip de computador.

Simples: A informação também deve ser simples, não excessivamente complexa. Informação sofisticada e detalhada pode sobrecarregar o conjunto de informações. Quando um tomador de decisão dispõe de muita informação, há dificuldade em determinar qual delas é realmente importante.

Pontual: Informação pontual é aquela obtida quando necessária. Por exemplo, as condições do tempo para a ultima semana não interferirão na escolha do vestir hoje.

Verificável: A informação deve ser verificável. Isso significa que você pode conferir-la e se assegurar de que está correta, talvez confrontando muitas fontes para uma mesma informação.

Acessível: A informação deve ser facilmente acessível aos usuários autorizados. Obtê-la na forma correta e no tempo certo atenderá, certamente, a suas necessidades.

Segura: A informação deve ser seguida para possibilitar seu acesso apenas pelos usuários autorizados.

Com essas características, as informações de uma organização servirão de insumo para vantagens competitivas e deixarão de ser algo inerte e sem funcionalidade empresarial, para se transformarem em recurso de significativo valor.

Com a valorização da informação e o reconhecimento de seu potencial competitivo, surge a necessidade cada vez mais de ações que visem a sua segurança. Na próxima seção serão abordadas questões de segurança da informação.

3. PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando o risco ao negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR/17999, 2005).

Pemble (apud MARCIANO, 2006) sugere que a segurança da informação seja definida em termos das atribuições do profissional responsável por ela. O autor descreve três esferas de atuação desses profissionais em torno das quais a segurança deve ser parametrizada e compreendida:

- a esfera operacional, voltada ao impacto que os incidentes podem gerar à capacidade da organização de sustentar os processos do negócio;
- a esfera da reputação, voltada ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário;
- a esfera financeira, voltada aos custos em que se incorre na eventualidade de algum incidente.

Considerando a informação o principal patrimônio de uma empresa, como afirma Santos (2004) torna-se imprescindível maior atenção para as informações empresariais além de políticas de segurança da informação amplas que possibilitem prever toda vulnerabilidade a que está sujeita a informação de uma instituição.

Vários são os fatores de risco para a informação, dentre os quais se pode destacar: agentes físicos, tais como incêndios, inundações, terremotos, etc., que podem levar à perda física dos registros informacionais; agentes biológicos, como a alta temperatura, umidade e insetos, que danifica o suporte, causando a perda parcial ou total da informação; agentes humanos e tecnológicos, que, segundo Bernstein *et al.* (apud CARVALHO, 1996), podem ser enumerados como se segue:

1. A espionagem (*sniffers*) pela captação de todo o tráfego de informações que passa pela rede;
2. O disfarce (*spoofing* de IP – Internet Protocol) através de exploração de falhas no protocolo de rede;
3. Execução de aplicações não autorizadas (por exemplo, "cavalos de tróia") que podem produzir resultados indesejáveis como perda ou repasse de informações;
4. Repúdio ou negação de participação em transações;
5. Negação de serviço, como tirar um servidor do ar, por exemplo;
6. Exploração de senhas, através de tentativas de acesso ou exploração do arquivo de senhas; e
7. Engenharia social, técnica que utiliza a psicologia para obter informações dos próprios funcionários da empresa vítima utilizando a confiança adquirida com os mesmos.

Contudo, observa-se que as políticas e procedimentos de segurança da informação têm por objetivo assegurar que os benefícios oriundos do uso da informação sejam apenas da empresa a que pertence o direito de seu uso.

A análise do custo benefício, onde se estuda a necessidade de gastos com a proteção da informação é necessária, verificando se a informação custa menos que os gastos que serão destinados à sua proteção.

A política de segurança da informação, conforme a norma NBR/17799 (2005), "tem como objetivo prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as regulamentações relevantes". Ainda conforme essa norma, a segurança da informação pode ser caracterizada pelo uso de três fatores (NBR/17799, 2005):

- Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- Integridade: exatidão, completeza da informação e dos métodos de processamento;
- Disponibilidade: garantia de que os usuários obtenham acesso à informação e aos ativos correspondente sempre que necessário.

Portanto, com vistas a possibilitar a eficácia de uma política de segurança da informação é preciso que os fatores discriminados acima sejam plenamente atingidos.

Sabe-se que de diversas formas as políticas e diretrizes de segurança da informação sofrem ataques. A Engenharia Social, cujas características serão objeto de estudo da 4ª seção constitui-se em um recurso utilizado para fragilizar a segurança da informação gerada pelas empresas.

4. ENGENHARIA SOCIAL

A Engenharia Social é uma entre as diversas ameaças contra as políticas de segurança da informação e, em geral, talvez seja a menos notada quando se traçam políticas de segurança da informação. No entanto, deveria ser considerada como uma prioridade, tendo em vista que é a porta de entrada para todos os demais ataques.

Para uma melhor discussão vale trazer algumas definições de Engenharia Social. Santos (2004) define a Engenharia Social como sendo:

> A arte de trapacear, construir métodos e estratégias de enganar em cima de informações cedidas por pessoas ou ganhar confiança para obter informações, são ações antigas, oriunda

> dos tempos mias remotos, ganharam um novo termo: Engenharia Social. (...) Engenharia por que constrói, em cima de informações táticas de acesso a sistemas e informações sigilosas, de forma indevida. Social por que se utiliza de pessoas que trabalham e vivem em grupos organizados.

Já KONSULTEX (apud ARAÙJO, 2005) trata a Engenharia Social como ciência que:

> (...) estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas da engenharia social são completamente utilizados por detetives (para obter informações), e magistrados (para comprovar se um declarante fala a verdade), também é utilizado para lograr todo tipo de fraudes inclusive invasão de sistemas eletrônicos.

A Engenharia tem como agente o engenheiro social que é quem a pratica tendo em vista o mesmo possuir a habilidade de enganar pessoas. Para atingir seu objetivo é sempre muito simpático e solícito de forma que a vítima, na maioria das vezes, não percebe que está sendo enganada e que acabou de contribuir com um invasor.

O engenheiro social usa de diversos artifícios previamente estudados para obter êxito nas suas investidas. Adota como estratégia de ação trabalhar as informações de caráter considerado inofensivo que obtém por meio de ataques a pessoas mal instruídas que, por sua vez, se tornam chave de entrada para outras informações mais relevantes.

Os ataques podem ocorrer através de contatos telefônicos, simulando um serviço de forma a obter informações que deseja; contatos através de e-mails falsos; contatos pessoalmente; verificação de lixo de escritório; e acesso indevido a ambientes de escritório.

Comer (apud SANTOS, 2004) afirma que geralmente as pessoas são o ponto mais suscetível em um esquema de segurança. Um trabalhador malicioso, descuidado ou alheio à política da informação de uma organização pode comprometer até a melhor segurança da informação.

O uso de recursos tecnológicos nas políticas de segurança da informação exige a presença imprescindível dos recursos humanos responsáveis que são pela força de trabalho da instituição. Santos (2004) afirma que "[...] deixar as pessoas desinformadas sobre as questões de segurança pode expor uma organização a riscos desnecessários, uma vez que os 'invasores' utilizam a habilidade de enganar os usuários para promoverem os ataques aos sistemas de informação dessas organizações".

A divulgação dos procedimentos corretos sobre segurança de informação, o alerta de

como se caracteriza um ataque do engenheiro social e a capacidade de observação por parte dos funcionários são o caminho correto para se alcançar resultados eficazes no combate à nocividade provocada por esses profissionais à segurança da informação gerada pelas instituições.

As UIAs têm como função básica tornar disponíveis as informações registradas independente do seu suporte. Os profissionais da informação prezam pela rápida recuperação da informação, assim como a sua integridade, acessibilidade, confidencialidade e exatidão. São nas UIAs que se encontram as informações necessárias para o desempenho das atividades da empresa. Portanto, cabe às mesmas darem o suporte necessário ao melhor aproveitamento das informações disponíveis nos diversos setores da empresa.

Segundo Greewood (apud BRAGA, 1996),

> A informação é considerada como o ingrediente básico do qual dependem os processos de decisão, mas se, por um lado, uma empresa não funciona sem informação, por outro, é importante saber usar a informação e aprender novos modos de ver o recurso informação para que a empresa funcione melhor, isto é, para que se torne mais eficiente. Assim, quanto mais importante for determinada informação para as necessidades da empresa, e quanto mais rápido for o acesso a ela, tanto mais essa empresa poderá atingir os seus objetivos.

O universo empresarial é um sistema aberto que se alimenta de insumos informacionais internos e externos e pode-se considerar as UIAs como parte imprescindível na vida desse sistema, tendo em vista que é onde se encontra o registro das ações administrativas realizadas pelos seus funcionários.

Sem hesitar, a realização das atividades clássicas da administração – prever, organizar, comandar, coordenar e controlar – não será possível, como afirma Belloto (2004), sem a materialização da informação. A constatação feita por Bellotto (2004) remete para a necessidade da existência no quadro de funcionários de qualquer empresa da presença de um profissional da informação tendo em vista o mesmo ser responsável pela gestão da informação de tal empresa.

Atualmente, percebe-se que a informação ganhou um espaço importante nas organizações. Essa valorização não é por acaso, como afirma Santos e Santana (2002):

> São vários os fatores que têm alimentado o forte crescimento pelo interesse em identificar, registrar e utilizar o conhecimento que as organizações possuem, sendo que dentre os

> principais se destacam os resultados da reengenharia, o grande aumento da concorrência e os avanços na tecnologia da informação.

A informação não somente atrai olhares da empresa possuidora da informação, mas também de terceiros que interessados nesse valor informacional buscam de várias formas o acesso à mesma.

A seguir serão discutidas as formas de ataque do engenheiro social nas UIAs – que, na maioria das vezes, não é percebido – e a importância da conscientização de profissionais da informação que desenvolvem atividades nas UIAs, com vistas a criar nos mesmos a capacidade de anteciparem-se a tais ataques.

5. UNIDADES DE INFORMAÇÃO ARQUIVÍSTICA: CAMPO DE ATUAÇÃO DO ENGENHEIRO SOCIAL

Na empresas as UIAs têm seu sistema de gestão da informação estruturada com base nos seguintes procedimentos técnicos, como descreve Robere (apud JARDIM, 1999):

- Entrada:
    - Documentos produzidos e recebidos;
    - Informação não organizada.
- Tratamento:
    - Arquivamento;
    - Classificação;
    - Descrição;
    - Indexação;
    - Utilização;
    - Transferência;
    - Recolhimento (ocorre apenas em arquivos público);
    - Eliminação.
- Saída:
    - Informação organizada;
    - Dossiês.

A maioria das informações empresarial se encontra nas UIAs, onde são tratadas e muitas vezes mantidas por longos períodos de tempo. Marcondes [19--?] salienta que:

> A integridade e a disponibilidade das informações também podem ser prejudicadas por erros humanos, e isso corre quando não há treinamento adequado aos funcionários, ou ainda quando o mesmo está desmotivado em relação à organização onde trabalha. A falta desses treinamentos facilita, por exemplo, a engenharia social, onde os funcionários são enganados por telefone ou e-mail's, e são induzidos a práticas que prejudicam a informação.

Neste contexto, a conscientização dos profissionais da informação que atuam em UIAs sobre políticas de segurança da informação se faz cada vez mais necessária.

A Engenharia Social é uma prática silenciosa de roubo da informação. As UIAs, pelo seu caráter informativo, é um grande alvo de ataques dos engenheiros sociais. Hoje já se sabe que os ataques do engenheiro social são cada vez mais premeditados e resultado de muitos estudos até chegar à ação do ataque. Algumas situações que colocam em risco a segurança da informação nas UIAs das empresas são listadas como se segue:

- Atendimento via telefone, onde o engenheiro social se passa por alguém que não é, como por exemplo, se passando por um funcionário usuário da unidade de informação;
- Documentos sigilosos espalhados pela mesa, podendo o engenheiro social ler as informações contidas em tais documentos, enquanto conversa com o funcionário assuntos previamente analisado com objetivo de obter a atenção total do funcionário. Além disso, tal situação deixa o documento mais sucessível a furto pelo engenheiro social e expõe o documento a riscos biológicos;
- Pessoalmente, usando o poder de persuasão e a habilidade em enganar, o engenheiro social convence os funcionários a fornecerem informações de caráter sigiloso e/ou observa a digitação de códigos de acesso e senhas;
- Varredura de lixo de escritório, visto que muitas das informações descartadas no lixo podem conter insumos ao engenheiro social para ataques mais significantes ou até mesmo conter informações sigilosas que não foram eliminadas de maneira correta.

Peixoto (2006) afirma ainda que,

> O que o engenheiro social nada mais faz é simplesmente adquirir primeiro esta confiança para que depois de reforçado esse "vínculo" de amizade criado, possa então atacar e conseguir as informações. Ele prepara toda a teia de situações que pode vir a ocorrer, como questionamentos

> e perguntas das quais ele possa ter que responder no ato, sem gaguejar ou demonstrar insegurança, a ponto da vítima não ter motivo de desconfiar de algo estranho nessa conversa.

Adquirindo a confiança dos funcionários, torna-se mais fácil para o engenheiro social atingir o objetivo de apropriar-se de informações sigilosas, uma vez que o funcionário em questão não irá desconfiar de seu suposto "amigo".

A educação e a formação para os profissionais, seja de qualquer nível hierárquico, que atuam nas UIAs se fazem necessárias. Neste contexto, Araújo (2005) considera os treinamentos e conscientização controles preventivos de ataques contra as políticas de segurança da informação.

6. CONSIDERAÇÕES FINAIS

Com a informação atingindo cada vez mais *status* no ambiente empresarial, a relação da informação com a instituição a que pertence cada vez mais se baseia no seu valor.

As UIAs, são responsáveis pelo tratamento da informação para facilitar e agilizar as tomadas de decisões dos funcionários que atuam nas empresas. Cada vez mais os profissionais da informação dos arquivos devem observar a importância de políticas de segurança da informação dentro das UIAs – políticas que envolvam todo o fazer técnico, com medidas que buscam resguardar as informações, de extravio ou de acesso indevido.

O planejamento de ações de segurança de informação deve ser uma atitude indispensável à ação do arquivista enquanto gestor de uma UIA. Portanto, alocar recursos tecnológicos, humanos e materiais para assegurar a integridade da informação não pode ser considerado como um desperdício para a empresa porque a informação gerenciada de forma correta é garantia de sucesso para quem a usa.

No entanto, apenas alto investimento em recursos tecnológico não é suficiente para implantar políticas de segurança da informação eficiente. Normalmente os responsáveis pela tomada de decisão nas empresas preocupam-se em investir na a tecnologia porque entendem que a mesma por si só será capaz de resolver o problema dos ataques dos cientistas sociais. Porém, os sistemas de segurança só redundarão em custo-benefício para as empresas desde que gerenciados competentemente por profissionais da informação e pelos funcionários das UIAs.

A Engenharia Social e os demais ataques contra as informações empresariais só são possíveis de serem combatidos a partir do momento em que as empresas usarem como ferramentas a educação e a conscientização dos seus funcionários.

As formas de se educar e conscientizar os funcionários sobre a importância da segurança da informação podem se dar através do uso de teatro, campanhas com premiação, distribuição de cartilhas educativas, uso de estratégias do endomarketing, gincanas e palestras com brindes.

Conclui-se que são as pequenas atitudes que fazem toda a diferença na proteção da informação nas UIAs e só através da educação e da conscientização será possível alcançar eficácia no combate ao engenheiro social e às demais formas de ataque contra a segurança da informação empresarial.

REFERÊNCIAS

ARAÚJO, Eduardo Edson de. **A vulnerabilidade humana na segurança da Informação**. 2005. Monografia (Bacharel em Sistema de Informação) – Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais, Uberlândia, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes: tratamento documental**. 2.ed. Rio de Janeiro: FGV, 2004.

BERGMANN, Helenice Barcellos. **Programa GESAC: Olhares e espaços sobre a inclusão digital no Espírito Santo**. II ONLINE Conference OCS. Disponível em: <http://www.cibersociedad.com/congres2004/grups/fitxacom_publica2.php?grup=29&id=616&idioma=en>. Acesso em: 5 nov. 2005.

BRAGA, Ascenção. A gestão da informação. **Millenium on.line**, [S.I], n.19, 2000. Disponível em: <http://www.ipv.pt/millenium/19_arq1.htm>. Acesso em: 05 maio 2008.

CARVALHO, Fábio Câmara Araújo de. et al. **Abordagem de sistema de informação enfocando a segurança em ambientes Internet/intranet/extranet. Florianópolis**.[s.d.]. Disponível em: <www.abepro.org.br/biblioteca/ENEGEP1999_A0569.PDF>. Acesso em: 04 de abr 2008.

CRUZ, Edilson Fernandes da. **A proteção do conhecimento sensível no terceiro milênio**. Palestra apresentada no I Simpósio Regional de Proteção ao Conhecimento. Rio de Janeiro, 5 de novembro de 2001.

JARDIM, José Maria. **Transferência e opacidade do estado no Brasil**. Niterói: EdUFF, 1999.

LATRES, Helena Maria Martins; ALBAGLI, Sarita. Chaves para O terceiro Milênio na Era do Conhecimento. In: ____. **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campos: 1999, p.8.

LOPES, Luis Carlos**. A nova arquivística na modernização administrativa**. Rio de Janeiro: [s. n.], 2000.

MARCIANO, João Luiz Pereira; LIMA-MARQUES, M. O enfoque social da segurança da informação. **Ciência da informação**, Brasília, v. 35, p. 89-98, 2006.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

OLIVEIRA, Djalma de Pinto Rebouças de. **Sistemas de informações gerenciais:** estratégicas, táticas, operacionais. 4° ed. São Paulo: Atlas, 1997, p.34.

PEIXOTO, César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: BRASPORT, 2006.

SANTOS, Luciano Alves Lunguinho. **O impacto da engenharia social na segurança da informação**. 2004. Monografia (Pós-graduação em redes de computadores) – Universidades Tiradentes, Aracaju, 2004.

SANTOS, Plácida L. V. Amorim da Costa; SANT'ANA, Ricardo César Gonçalves. Transferência da Informação: análise para valoração de unidades de conhecimento. **DataGramaZero:** Revista de Ciência da Informação. Rio de Janeiro, v.3, n.2, 2002. Disponível em: <www.dgz.org.br/abr02/Art_02.htm>. Acesso em: 12 abr 2008.

SMICALUK, Adriana. Et al. Política de Segurança da Informação. **Orlei José Pombeiro**, [S.I], [s.d]. Disponível em: <www.orleijp.eng.br/CompSociedade>.Acesso em 06/05/2008.

STAIR, Ralph M.; REYNOLDS, George W. Uma introdução aos sistemas de informação. In._____ **Princípios de sistemas de informação**: Uma abordagem gerencial. 4° ed. Rio de janeiro: LTC, 1999.

TAKAHASHI, Tadao. **A Sociedade da Informação**. In: BRITES, Juçara e PERUZZO, Cicília (orgs.): Sociedade da Informação e Novas Mídias: participação ou exclusão? São Paulo: Intercom, 2002.

TONINI, Regina santos Silva. **Custo na gestão da informação**. Salvado: PETROBRAS, 2006, p. 23.