FUNDAÇÃO GETÚLIO VARGAS

CURSO DE ESPECIALIZAÇÃO EM ADMINISTRAÇÃO PÚBLICA

DENISE MONTEIRO DE SOUZA SILVA

REDUZINDO OS IMPACTOS COM OS USUÁRIOS, NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE TI

2009

DENISE MONTEIRO DE SOUZA SILVA

REDUZINDO OS IMPACTOS COM OS USUÁRIOS, NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE TI

Projeto apresentado à Fundação Getúlio Vargas, como requisito parcial para a aprovação na disciplina Introdução ao Trabalho Científico do Curso Intensivo de Pós-Graduação em Administração Pública

BELO HORIZONTE

2009

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

Nos últimos anos, tem havido uma rápida evolução das tecnologias de informação e comunicação. O baixo custo de aquisição de computadores, a popularização do acesso à Internet e o grande desenvolvimento de sistemas via WEB, tem mostrado a grande vulnerabilidade das organizações quando se trata de manter seguras as suas informações.

Ameaças aos sistemas de informação e rede de dados podem acarretar um enorme prejuízo para as empresas. Invasões, roubos eletrônicos, páginas web alteradas, hackers, vírus, spam são alguns temas que passaram a fazer parte do nosso dia-a-dia. Neste contexto, a Segurança da Informação é um assunto que muito tem sido falado e é também objeto de preocupação nas empresas que têm na informação um ativo de negócios valioso e sabem que deve ser protegido.

Fazer investimentos em recursos tecnológicos para se proteger destas ameaças faz parte da preocupação e responsabilidade das empresas quando estas se dispõem a utilizar recursos virtuais. Mas apesar dos avanços não existe solução 100% segura. Soluções tecnológicas sozinhas não garantem a segurança da informação na organização, pois a grande maioria dos problemas de segurança são gerados por pessoas, pois são elas que estão no comando, operam sistemas, abrem e-mail, acessam sites, geram documentos. As inúmeras possibilidades de acessos às informações num ambiente Web, por exemplo, aumentam a curiosidade das pessoas que, estimuladas por mensagens, fotos e clicks correm riscos muitas vezes sem nem ao menos saberem ao que estão se expondo.

Com base nestas ações de risco a que as pessoas se expõem e muitas vezes expõem também toda a organização cada vez mais as empresas vêm se preocupando em definir uma

Política de Segurança da Informação, visando normatizar e definir um comportamento seguro dentro do ambiente de TI.

Ter uma Política de Segurança da Informação hoje em dia significa evitar problemas e minimizar riscos e formalizar a delegação, direitos, restrições, obrigações, responsabilidades e penalizações. Estes pontos são fundamentais na elaboração de uma boa política de segurança e esta não é uma tarefa simples, pois o principal risco de segurança está no comportamento das pessoas.

A implantação de uma política de segurança quase sempre incomoda a maioria dos usuários que até então estavam acostumados a liberdade total num ambiente sem regras e limites. Normalmente estes tentam criar resistência à implantação das políticas de segurança, quando não tentam violar as regras estabelecidas.

Se não houver adesão e apoio da alta direção à implantação de uma PSI, esses serão os primeiros a solicitar a concessão de exceções, sendo então os primeiros a não cumprirem as normas de segurança.

Mesmo sem usar de recursos tecnológicos, muitas pessoas usam de algum privilégio ou da ingenuidade ou descuido das pessoas para conseguirem informações confidenciais. Uma tela de computador aberta com documento confidencial, papéis importantes jogados no lixo ou simplesmente anotações deixadas em cima de uma mesa. É o que chamamos de engenharia social.

Investir em tecnologia é muito importante para se aplicar as regras de segurança e monitorar seu cumprimento, identificar as ameaças e riscos, mas se as pessoas não forem devidamente conscientizadas no entendimento da política de segurança e na responsabilidade de suas ações e da importância da sua participação, teremos aí um alto nível de insatisfação e situações de risco.

A gerência da segurança com foco nas pessoas está baseada em regras de segurança e no seu monitoramento.

Uma política de segurança deverá especificar formal e claramente as regras a serem seguidas pelas pessoas para acessarem os recursos e as informações da empresa.

A alta direção das empresas em sua maioria se esquece que, não basta criar as regras e impô-las aos seus usuários. A "cultura de segurança" é todo um aprendizado que deve ser adquirido e este conhecimento deve ser repassado pela empresa aos seus usuários para que os mesmos tenham comportamentos seguros assim como quando vão atravessar uma rua no semáforo verde para pedestres ou saem de casa e trancam a porta para que um estranho não entre. A verdade é que não estamos livres ser atropelados simplesmente porque atravessamos a rua no sinal verde para pedestres, como também não evitamos um assalto só porque trancamos a porta de casa. Mas devemos conhecer os perigos, os riscos a que estamos sujeitos para que possamos agir com segurança e dificultar a ocorrência destes incidentes ou minimizar os seus prejuízos.

Como implantar uma política de segurança da informação e ao mesmo tempo reduzir a resistência e a insatisfação dos usuários?

Palavras chave: Segurança da Informação, Política de Segurança da Informação - PSI, Incidente de Segurança, Cultura de Segurança, Treinamento.

1.2 Objetivos

Este estudo terá como foco fazer uma compilação do que relatam alguns autores cujas experiências de implantação de uma PSI obtiveram sucesso, e ainda identificar as ações mais importantes na implantação de uma política de segurança da informação no ambiente de TI

para criar uma “cultura de segurança” levando conhecimento aos usuários de tal maneira que faça com que o comportamento dos mesmos contribua para o sucesso da sua implantação, reduza a insatisfação e minimize os riscos para os negócios da empresa.

1.2.1 Objetivos finais

- Reforçar a idéia de que é extremamente necessário investir em pessoas para que, uma Política de Segurança da Informação seja implantada com sucesso.

1.2.2 Objetivos intermediários

- Expor o conceito de segurança da informação.
- Expor o conceito de política de segurança da informação.
- Expor práticas, recomendações e normas básicas de implantação de uma PSI.
- Identificar as principais falhas na implantação de uma PSI.
- Identificar os principais fatores culturais de uma organização que contribuem para impactar a implantação de uma PSI.
- Identificar os pontos principais de apoio que garantem o sucesso de implantação de uma PSI.
- Identificar as principais ações que podem transformar as pessoas em parceiras, responsáveis pela implantação de uma PSI e o cumprimento de suas normas.
- Casos de sucesso onde o investimento em campanhas de divulgação, treinamento e capacitação trouxeram resultados positivos.

1.3 Relevância do Estudo

Este estudo torna-se relevante, pois pretende a partir da leitura de vários autores e publicações, mostrar que existe um entendimento por parte dos mesmos de que, a necessidade de reduzir os impactos com os usuários na implementação de políticas de segurança para que a mesma obtenha sucesso e alcance seus objetivos, passa pela prioridade de se fazer investimentos no treinamento, capacitação e campanhas de conscientização de todos os usuários do ambiente de TI.

2 REFERENCIAL TEÓRICO

2.1 O que é segurança da informação no ambiente de TI

A norma ABNT NBR ISSO/IEC 17799:2005 define informação como sendo *"um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida"*. Nesta mesma norma segurança da informação é definida como sendo *"a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio"*.

Para que se garanta a proteção da informação, ações devem ser implementadas de tal forma que reduzam os riscos com vazamentos, fraudes, erros, uso indevido, sabotagem, roubo de informações entre outros incidentes que possam comprometer os negócios da organização. Como conseqüência da aplicação destas ações, também deverá aumentar a produtividade dos usuários, pois o ambiente de TI ficará mais organizado, padronizado e com regras.

Normas são padrões definidos a serem seguidos por todos os usuários, para que práticas efetivas de comportamento consciente e seguro garantam a segurança da informação. Políticas são intenções e diretrizes a serem seguidas.

Na elaboração de uma política de segurança os objetivos devem estar claros e mensuráveis para que sua implementação através das normas possam ser seguidas por todos.

A segurança da informação deve ter como visão *"Fazer com que a segurança permeie a vida das organizações, impactando da menor forma possível a sua rotina, mantendo os riscos dentro dos patamares desejados." (Security Officer-2006, página 37).*

A segurança da informação tem como premissas três paradigmas básicos:

Integridade: A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas. A manutenção da integridade pressupõe a garantia de não violação das informações seja ela acidental ou proposital.

Confidencialidade: Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal.

Disponibilidade: Característica da informação que se relaciona diretamente a possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas atividades. Garante que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para processos ou pessoas autorizadas.

Há ainda que se considerar outros atributos como os citado por Laureano (2005)

> *"Outros autores (Dias, 2000; Wadlow, 2000; Shirey, 2000; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002; Sêmola, 2003; Sandhu e Samarati, 1994) defendem que para uma informação ser considerada segura, o sistema que o administra ainda deve respeitar:*
>
> *• **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exatidão, a origem do dado ou informação;*
>
> *• **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;*
>
> *• **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.*
>
> *• **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste é caso é atribuído o caráter de*

confidencialidade a informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

*• **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança."*

2.2 Política de Segurança da Informação.

A Política de Segurança da Informação atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham. Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não a cumprirem.

A elaboração e implantação de uma PSI em uma organização deverão estar baseadas em padrões e normas internacionais como (TECSEC, 1985), (ISO 15408:1999), (ISO/IEC TR 13335:1998), (BS7799-2:2001), (ISO/IEC 17799:2005), (ISSO/IEC27001:2005), (IEC 61508:1998).

A aplicação de uma metodologia para implantação de um sistema de gerenciamento da segurança da informação resultará na padronização e documentação dos procedimentos, utilização de ferramentas e técnicas adequadas, além da criação de indicadores, registros e da definição de um processo educacional para capacitação, treinamento e conscientização da organização envolvida. Todas estas ações deverão promover a mudança de cultura necessária para o cumprimento satisfatório da PSI.

Conforme citado em Benz (2008)

> *"Os fatores que determinariam o sucesso da segurança da informação numa organização, segundo ABNT/ISSO 17799:2005(ABNT, 2005) são:*
>
> *-Política de Segurança da Informação, objetivos e atividades que reflitam os objetivos do negócio;*
>
> *-Uma abordagem e uma estrutura para implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;*
>
> *-Comprometimento e apoio visíveis de todos os níveis gerenciais;*
>
> *-Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação dos riscos e da gestão de risco;*
>
> *-Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;*
>
> *-Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;*
>
> *-Provisão de recursos financeiros para as atividades de gestão da segurança da informação;*
>
> *-Provisão de conscientização, treinamento e educação adequados;*
>
> *-Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;*
>
> *-Implementação de sistema de medição que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para sua melhoria".*

2.3 Incidentes de segurança – comportamento de risco

Tudo que possa por em risco as atividades da empresa são considerados ameaças e se ocorridos, são incidentes de segurança.

> *"Um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação". [ISO/IEC TR 18044:2044*].

Os incidentes de segurança ocorrem em diversos níveis dentro de uma organização e para cada nível (estratégico, tático, operacional) o tratamento tem que ser apropriado.

Segundo Benz (2008)

> *"Os autores prosseguem sugerindo que não há espaço pra complacência na aplicação da política de segurança, que deve permear toda a organização; as pessoas precisam realmente ser conscientizadas da sua importância". [] "A*

> *necessidade da implantação de uma "consciência de segurança da informação" é referida por Kruger e Kearney (2006) com base no argumento de que a gestão efetiva da segurança da informação requer uma combinação de controles técnicos e de procedimentos: o valor destes controles usualmente depende da sua implementação e uso corretos, ambos realizados por pessoas. Assim, a implementação de controles de segurança efetivos depende da criação de um ambiente positivo de segurança, onde todas as pessoas realmente compreendam e adotem os comportamentos que delas são esperados."*

Atitudes como:

- Abusos no uso de correio eletrônico;
- A ameaça de engenharia social;
- Propriedade intelectual;
- Vazamento de informações através de mídias, e-mail, pen-drives;
- Vazamento e compartilhamento de senhas;
- Descuido com o crachá/cartão/documentos da empresa,

São alguns dos fatores geradores de problemas com a segurança da informação.

Conforme citado em Laureano, (2005)

> *"Todas as informações (ou quase) têm a interferência de um ser humano no processo ou tecnologia, neste caso é necessário garantir a confiabilidade humana nas partes envolvidas. No contexto da engenharia, a confiabilidade humana é a probabilidade de que um humano execute corretamente uma tarefa designada em um tempo especificado, durante um período de tempo definido em um ambiente também especificado (Lasala, 1998)". [] "Alem disso, (Peixoto 2005) afirma que o fator humano está presente no sucesso ou no fracasso da maioria dos episódios que envolvem segurança ou problemas de segurança da informação, devendo esse aspecto da segurança merecer atenção especial".*

2.4 Pessoas o elo mais fraco – um problema cultural

O foco de uma PSI é sempre garantir a continuidade dos negócios da empresa por este motivo ela não é elaborada para dar continuidade ao que já está ela promove mudanças, restringe a liberdade de ação e na maioria das vezes desagrada aos usuários de TI.

"A origem dos problemas de segurança podem ser, basicamente, divididas em três categorias: natural, acidental ou intencional, sendo as duas últimas relacionadas com o fator humano." (Security Officer 2006, página 27)

> *"Alguns dos principais problemas relativos às pessoas na implementação de mudanças organizacionais intencionais, identificados na literatura, têm sido as dificuldades de: comunicação dos objetivos definidos pela organização; compreensão desses objetivos pelos indivíduos; promover-se o trabalho em equipe; fazer com que os indivíduos adotem a mudança." (Silva e Vergara)*

De acordo com Benz (2008),

> *"Da mesma forma, estes mesmos estudos apontam como principais fatores inibidores deste tipo de alinhamento, a falta de apoio visível da diretoria (PELTIER,2002); a divulgação ineficaz da segurança junto aos funcionários e/ou treinamento inadequado (PELTIER,2002); e a falta de um programa de medição da eficácia do controle (PELTIER,2002)".*
>
> *"A opinião prevalece entre os administradores de segurança, como o responsável pelo setor na Companhia Energética de Minas Gerais (Cemig), José Luís Brasil, para quem "a engenharia social existe porque as empresas investem em tecnologia e esquecem as pessoas. São elas que operam sistemas e máquinas, que fornecem informações. Se elas não sabem por que estão apertando um parafuso, não sabem a importância do seu trabalho, passam a ser um ponto fraco no processo ". (Revista Fonte pag. 15 – artigo: Privacidade Integridade e Sigilo - Os desafios da segurança da informação)*

Em seu estudo Smicaluk, faz também uma importante conclusão que vem reforçar que, pessoas podem por em risco todo o negócio da empresa e por este motivo devem ter atenção especial.

> *"Os estudos mostraram que existem atualmente muitas ameaças que atingem diretamente as empresas e suas informações como as ameaças naturais causadas por enchentes e incêndios, e até mesmo ameaças criadas ou causadas por pessoas mal intencionadas, como vírus e hackres, o que obriga essas empresas a implementação de Política de Segurança para proteger seus dados de possíveis falhas e ataques. Todas as ameaças citadas anteriormente alem das discussões obtidas em sala nos mostraram que na maioria das vezes, as informações das empresas entram em risco não somente através dessas ameaças, mas sim através de seus próprios usuários, que desinformados, despreparados ou até mesmo mal intencionados acabam sendo a principal fonte de disseminação de vírus e de comprometimento de informações das empresas o que as leva na maioria das vezes ao fechamento. E para que isso não ocorra seria necessário, além das ferramentas de proteção, um foco maior no usuário, dando a ele treinamento, informações e o conscientizando para que não cometa erros que possam comprometer todas as informações da empresa. "*

As principais as falhas organizacionais, em relação ao comprometimento com a segurança da informação, a PSI e com usuários de TI são:

- Não comprometimento da alta direção com a PSI. (Normalmente são os primeiros a pedir para terem tratamento diferenciado.)
- Falta de estruturação formal de uma hierarquia para cuidar da segurança da informação.
- Falta de destinação de recursos para ações conscientização, treinamento e capacitação dos usuários.

2.5 Investindo em Programas de conscientização, campanhas motivacionais e treinamento.

Uma vez feito os investimentos em tecnologia e com uma política de segurança elaborada e publicada, cabe agora cuidar em quem diretamente vai sentir as mudanças ocorridas a partir destas implementações: o usuário do ambiente de TI.

> *"Um bem sucedido programa de conscientização de segurança de TI deve mudar o modo como o usuário de sistema pensa e age, de forma que a segurança de TI torne-se parte das atividades de negócios da empresa. O Programa deve endereçar a todas as pessoas que tenham contato com sistemas computadorizados, porque para construir um nível consistente de segurança em todas as partes de uma organização é necessário não ter nenhum elo fraco na corrente." (Silva – 2005)*

Sem conhecer as normas da política de segurança da informação e treinamento o usuário não poderá ter um comportamento seguro.

> *"O treinamento não é simples. Não se padroniza o usuário. Enquanto uns têm acesso limitado, outros, em pontos superiores da escala de poder, têm acesso quase irrestrito. Enquanto uns estão bem acostumados aos recursos disponíveis, outros não têm o mínimo conhecimento e, muitas vezes, estão no topo da hierarquia. As regras para a presidência são permissivas e, na maioria das vezes, é onde estão os usuários menos preparados. Via de regra, desprezam treinamentos. Não que os achem desnecessários ou menos importantes, mas por não terem tempo a "perder" com estes treinamentos." (Revista Fonte Julho/Dezembro – 2007, pag.46/47- A chave da Segurança está no Treinamento - Erasmo Borja Sobrinho.)*

Torna-se importante neste momento, para consolidar a idéia deste trabalho, apresentar casos de empresas cuja implantação da PSI não negligenciou o usuário como peça fundamental para o sucesso.

Silva (2005) em seu estudo em que trata do Impacto na implantação de política de segurança da informação na Novo Nordisk Produção Farmacêutica do Brasil nos fala das etapas do programa de conscientização dos usuários onde foram definidos os objetivos, o foco, a mensagem, os materiais a serem produzidos, os custos, um cronograma e as ações do que ele chamou de Campanha 1, de programa de conscientização em TI e termina fazendo a seguinte conclusão sobre os resultados analisados após a implantação:

> *"De uma forma indireta, buscando trabalhar o comportamento dos usuários de sistemas, visto que uma das maiores falhas de segurança nas organizações está no fator humano, conseguiram-se resultados ligados diretamente à segurança. Apesar da empresa NNPFB possuir diversas tecnologias como suporte a segurança da informação, havia problemas como a disponibilidade dos sistemas, e ao se trabalhar o comportamento das pessoas esse problemas foi praticamente resolvido. De acordo com a avaliação da campanha pose-se constatar que uma campanha bem trabalhada, seguindo todas as etapas necessárias, e o principal, tendo o apoio da administração da empresa, é possível reduzir os riscos de segurança da*

informação da empresa. Mas é importante ressaltar a necessidade de se ter uma continuidade da campanha ou todo seu trabalho pode cair no esquecimento, e as falhas de segurança retornarem."

Ainda para referendar a importância dos investimentos em pessoas para que uma PSI seja seguida por todos os usuários e que estes estejam conscientes da importância da sua participação neste processo, abaixo são apresentados textos da Revista Fonte, Ano 4, número 07, Julho/Dezembro de 2007 uma publicação da Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE, edição cujo tema é Segurança da Informação, Tecnologia e comportamento na prevenção e combate aos crimes virtuais. Nestes textos através de depoimentos de pessoas que foram responsáveis pela implantação de programas de segurança em empresas de grande porte, percebe-se que foi dada aos usuários a devida atenção e por este motivo o projeto de implantação de PSI foi bem sucedido.

2.6 - Casos de sucesso

A seguir foram selecionados trechos de depoimentos de pessoas que foram responsáveis pela implementação de uma política de segurança em suas empresas. Estes depoimentos vêm reafirmar a importância dos investimentos em ações para capacitar e conscientizar seus usuários e o quanto estas ações foram responsáveis pelo sucesso da implementação.

- Cemig – Companhia Energética de Minas Gerais

"Desde 1993, a Cemig preocupa-se com a segurança de suas informações. Segundo o Coordenador José Luís Brasil, com o mainframe já se adotava a utilização de software de gestão da segurança, ainda de forma centralizada. Em 1996, houve a primeira iniciativa de implantação de uma política de segurança na Empresa, que, no entanto, figurou somente no Manual de Organização da Cemig, entendida como mais uma norma da Empresa. Essa política foi escrita para toda a corporação, não só para a área de TI. "Naquela época", lembra Luís Brasil, "nem todo o ambiente de TI operava em rede e a conexão com a internet estava longe de ser como hoje. Os riscos eram, portanto, menores".

Luís Brasil explica que o planejamento das capacitações considerou um fato importante: a grande dispersão da Empresa em todo o Estado. "Como podíamos estar juntos a todos os empregados? A Cemig tem sete regionais: Centro (em Belo Horizonte), Triângulo, Sul, Mantiqueira, Norte, Oeste e Leste. Pensávamos que esse trabalho deveria ser algo interessante, diferente". Foi contratado, então, o grupo de teatro empresarial Grafite, de Belo Horizonte, que criou roteiros personalizados com base nos temas fornecidos pela equipe da ASI. "Eles desenvolviam roteiros específicos e faziam uma apresentação prévia para nossa aprovação ou para adequações". Segundo Luís, houve uma receptividade muito boa. "O treinamento

> *era composto de palestras e das peças de teatro, que representavam cenas dos conteúdos abordados nas palestras. Reforçaram, dessa forma, conceitos de segurança da informação, engenharia social e políticas de segurança. A duração era de meio expediente e acontecia em ambientes da Cemig, com um custo médio de R$40,00 por empregado".*
>
> *"Nunca utilizamos imagens como cadeados, que remetem à exclusão, enfatizando, ao contrário, a segurança da informação com abordagem de inclusão; nunca como policiamento", ensina o coordenador do programa. Nenhum dos treinamentos é obrigatório.*
> *Com esse roteiro, chegaram a treinar 1.500 pessoas em um ano. "Cada vez mais procurávamos a inovação, sempre resguardando a preocupação de proporcionar um treinamento agradável, com brindes, jogos, brincadeiras e o teatro. "Sai barato para a empresa", garante. "" (Revista Fonte Julho /Dezembro-2007 pag. 38-39 artigo - Cemig Humor na construção de uma cultura de segurança)*

Pode-se observar pelo relato acima que o treinamento foi feito de uma forma lúdica, de tal forma a atrair o interesse do usuário para o tema e dessa forma conseguir obter o resultado esperado e com pouco investimento.

- SEPLAG – Secretaria de Estado Planejamento e Gestão de Minas Gerais

> *"A campanha de segurança da informação da Seplag utilizou como mote "Segurança da Informação. Adote essa idéia."... O processo de conscientização contou com a realização de 11 palestras de sensibilização com a peça teatral "As velhas e o dia de chuva", para 800 servidores públicos, contratados e estagiários. Essa peça teatral já havia sido utilizada pela Companhia Energética de Minas Gerais (Cemig) e aborda, de forma lúdica, os problemas dos velhos hábitos de segurança da informação adotados pelas pessoas. Nas palestras foram distribuídas cartilhas e brindes, como camisas, cordas de crachás e canetas.*
> *Na intranet da Seplag foi criada uma área de segurança da informação e foram divulgados 12 cartazes sobre o tema, ao longo do ano de 2006". Revista Fonte Julho/Dezembro/2007 pag 66.*

Conforme informações contidas em apresentação elaborada por Marconi Martins de Laia para participação no II Security Meeting sobre o Plano Corporativo de Segurança da Informação da Secretaria de Estado Planejamento e Gestão de Minas Gerais, sobre o processo de sensibilização em segurança da informação ele relata que foram implementadas as seguintes ações:

> *"- Palestras de sensibilização com peça teatral "As velhas e o dia de chuva" para 800 servidores públicos, estagiários e contratados.*
> *- Distribuição de uma cartilha de segurança e brindes.*
> *- Criação de uma área de segurança na intranet.*
> *- Divulgação de 12 cartazes sobre o tema segurança."*

Também notamos que na SEPLAG houve o interesse em criar um clima de descontração que atraísse o usuário com peças teatrais, distribuição de brindes e cartilha para fixação de temas importantes.

- Receita Federal

> *"O gerenciamento das ações de segurança da Receita está centralizado em Brasília, onde atua a coordenação de TI, com uma divisão de segurança da informação. Essa área é responsável pela normatização e disseminação das informações. Nas regionais, em todo o País, também existem divisões de TI. Cada unidade conta com estrutura própria, para supervisão geral da legislação e implantação.*
>
> *Os funcionários foram exaustivamente informados sobre o conceito e os riscos da engenharia social, por meio de campanhas de conscientização e disseminação e a publicação do Manual Institucional de Segurança, que contempla todos os aspectos relacionados ao tema, como software, engenharia social, controles de acesso. A Receita mantém ainda campanha permanente da intranet. "Hoje, o nível de consciência para TI é bastante alto, todos têm uma preocupação muito grande com a segurança. É um trabalho que não acaba nunca, não se pode dar trégua: são cartazes, alertas, palestras, filmes – é um trabalho permanente". Donizette ressalta que "o mais importante é o trabalho com as pessoas, as normas por si só não fazem nada acontecer. Depende das pessoas, de um trabalho de divulgação, de conscientização". Revista Fonte Julho/dezembro-2007, pagina 43*

Na Receita Federal podemos notar que, após o trabalho inicial houve preocupação permanente em manter o usuário conscientizado e informado.

3 Conclusão

Podemos concluir que existe realmente um ponto em que a maioria dos autores concorda e que ficou demonstrado com este estudo: é que uma PSI não cumpre o seu papel se não houver tratamento igual aos três pilares que a sustentam:

- Investimento em tecnologia

, a formalização das políticas, procedimentos e práticas de segurança se incluído aí ações de conscientização, treinamento e capacitação dos usuários.

De nada adianta investir em recursos tecnológicos e fazer publicar uma PSI só para formalizar e ficar em dia com as regras de segurança. As pessoas precisam ser preparadas para aceitar as mudanças, se adaptarem com menor impacto possível de tal maneira que a produtividade no trabalho fique garantida, elas trabalhem satisfeitas e sem por em risco a continuidade dos negócios da empresa.

Por mais que os interesses da empresa estejam em primeiro lugar, não devemos esquecer que são pessoas que vão concretizar este interesse. O que garante que tudo vai estar dentro do planejado, ser executado e transcorrer com segurança é o envolvimento das pessoas, se sentindo parte do processo e responsável por ele.

"O processo de segurança da informação envolve muitos elementos, mas com certeza o usuário é fundamental e devemos tratar com carinho." (Fontes – 2007)

REFERÊNCIAS

ANT NBR/ISO/IEC 17799:2005 Tecnologia da Informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

BENZ, Karl Heinz - Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas aditadas na TI: Estudos de casos em instituições financeiras – 2008 - Disponível em <http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=126310>, acessado em:12/08/2009

FONTES, Edison – Segurança da Informação: o usuário faz a diferença – 2007 - Disponível em <http://www.viaseg.com.br/artigos/artigo_edison_051125.htm> acessado em 09/08/2009.

LAIA, Marconi Martins de - Plano Corporativo de Segurança da Informação da Secretaria de Estado Planejamento e Gestão de Minas Gerais - 2006 - Disponível em <http://www.egov.mg.gov.br/Seguranca_da_informacao-11 - link Notícias 09/11/2006>, acessado em 18/06/2009

LAUREANO, Marcos Aurelio Pchek - Gestão de Segurança da Informação- 1/06/2005 Disponível em: < http://www.mlaureano.org/aulas_material/gst/apostila_versão_20.pdf>, acessado em: 07/08/2009.

REVISTA FONTE, ano 4, número 07, Julho/Dezembro de 2007 uma publicação da Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE - Segurança da Informação, Tecnologia e comportamento na prevenção e combate aos crimes virtuais.

SECURITY OFFICER - Guia Oficial para Formação de Gestores em segurança da Informação – Módulo Security Education Center 1ª Edição – 2006 - Revista Fonte – PRODEMGE – Edição de Julho/Dezembro – 2007

SILVA, José Roberto Gomes da; VERGARA, Sylvia Constant;
A Mudança Organizacional Pela Ótica dos Indivíduos: Resistência ou uma Questão de Sentimentos, Significado e Constituição do Sujeito? – Disponível em <http://www.anpad.org.br/eneo/2002/dwn/eneo2002-08.pdf>, acessado em: 30/07/2009.

SILVA, Valflávio Bernardes – Impacto na implantação de política de segurança da informação na Novo Nordisk Produção Farmacêutica do Brasil – 2005 – Disponível em <http://www.ccet.unimontes.br/arquivos/monografias/76.pdf>, acessado em 08/06/2009.

SMICALUK, Adriana; WILLE, Marcos Vinícius; ORLEI, Adriano Slisinsk; POMBEIRO, José - Política de Segurança da Informação - Disponível em <http://www.assespropr.org.br/uploadAddress/Politica_de_seguranca_da_informacao.pdf>, acessado em: 09/08/2009.