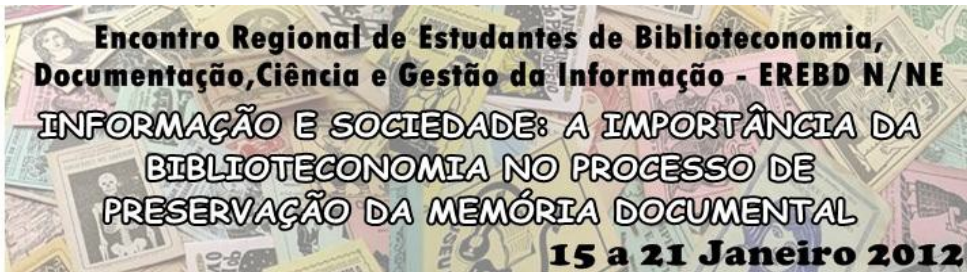


CONDUTAS DO FATOR HUMANO:
Alicerce da Segurança da Informação[1]

Acilégna Cristina Duarte Guedes Alcoforado[*]
Emerson da Cruz Ribeiro[**]
Jacqueline de Araújo Cunha[***]

Resumo: Discorre os meandros do fator humano e suas principais fragilidades no campo da segurança da informação. Aborda questões que colaboram quanto à proteção da informação e sua salvo conduta no decorrer de todo o processo até o receptor. Cita o comportamento gestor nestas unidades de informação e suas nuances internas às situações de riscos. Apresenta índices das mais recentes pesquisas no campo de segurança empresarial aos seus bancos de dados confidenciais e os níveis que mostram eficácia, referentes à proteção da informação no âmbito tecnológico, quanto a possíveis ameaças nas empresas e como deve ser eliminadas. Comenta situações baseados em casos reais, como a rede social Facebook, um das redes sociais mais conhecidas na atualidade e de como esse império social se desenvolveu no quesito segurança. Aponta os caminhos do sucesso e a genialidade de Steve Jobs, quanto a sua forma de gerenciamento da Apple, além dos cuidados básicos que possam colaborar e/ou evitar situações de risco numa corporação. Objetivou-se neste trabalho abordar variadas situações de risco eminente vivenciados pela sociedade atual no que concerne a temática da Segurança da Informação de forma a delinear um quadro geral do problema envolvendo o aspecto humano. Utiliza como metodologia a pesquisa online bibliográfica e de periódicos relevantes, fazendo citações pertinentes ao desenvolvimento do artigo. Conclui que, como em outras áreas profissionais que carrega em si uma estrutura mercadológica, é fundamental estar atento as novidades de mercado quanto à segurança e suas possíveis consequências em fatores de risco em tempos atuais.

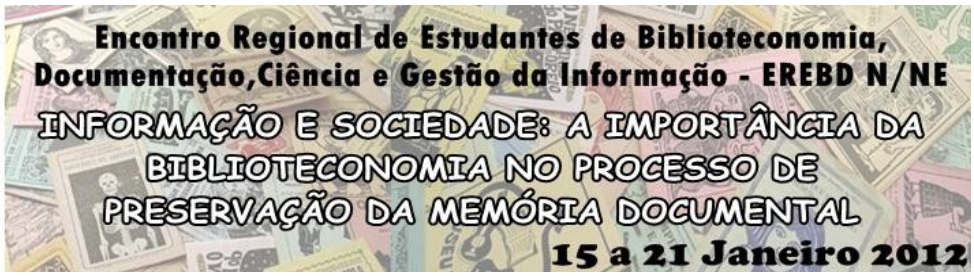
Palavras-Chave: Fator humano. Rede social. Situações de risco.

1 Comunicação Oral apresentada ao GT 06 – Tema livre.

* UFRN – Universidade Federal do Rio Grande do Norte / Campus Natal. Graduanda em Biblioteconomia. legnacris@gmail.com

** UFRN – Universidade Federal do Rio Grande do Norte / Campus Natal. Graduando em Biblioteconomia. mamutesound@hotmail.com

*** UFRN – Universidade Federal do Rio Grande do Norte / Campus Natal. Orientadora. Professora do Departamento de Biblioteconomia. jacquelinecunh@gmail.com



1. INTRODUÇÃO

Um conceito básico que define a Segurança da Informação de acordo com Beal (2005) é algo que resume um processo inerente a proteção de dados informacionais diante as possíveis ameaças quanto a sua integridade, disponibilidade e confiabilidade.

Diante do fluxo de informações e os novos suportes tecnológicos, sabe-se que a informação ganhou outro status ao que cabe sua disseminação. Com o advento da web e a velocidade vertiginosa de informações diversas ao que se refere a sua integridade e as formas de proteção tecnológicas, em algum seguimento informacional específico.

Através de mecanismos e planejamento eficazes, as empresas, sejam elas de pequeno a médio e/ou grande porte, investem em todo tipo de segurança: desde a sua estrutura física até os seus planos de diretrizes organizacionais.

Seguindo a premissa que *o segredo é a alma do negócio*, empresas apostam em suas idéias contando com o fator surpresa para sua concorrência. Daí o motivo principal para o sigilo absoluto em sua casta hierárquica numa empresa nos dias atuais. Pois qualquer vazamento de informações industriais ultra-secretas é capaz de arruinar um trabalho de meses ou até mesmo de anos numa fração de segundos.

Um dos exemplos mais recentes - que de inicio trazia uma idéia sem maiores pretensões, mas que virou algo grandioso - é o caso do Facebook, que se transformou numa das maiores redes sociais do mundo. Sendo que seu suposto criador Mark Zucherberg, foi acusado de se apropriar e registrar como sendo de sua própria autoria, o que seria a célula-mãe de um projeto, que depois valeria milhões de dólares. Além da própria segurança em si que o site de relacionamento por ele difundido, dispõe a seus usuários pelo mundo.

Em outro aspecto, temos em lado oposto o Steve Jobs que revolucionou o mundo com sua genialidade e empreendedorismo nos produtos da Apple e como o quesito da segurança da informação foi de extrema importância para a sobrevivência de suas idéias revolucionárias em um mercado deveras competitivo.

Sendo assim, podemos avaliar o peso do assunto e sua importância no nosso mundo globalizado, diante a gama de informações que nos chegam a todo instante. E como nós devemos nos portar frente a essas situações cotidianas que remetem algum perigo iminente.

Como meta para realizar o artigo, foi definida: analisar os aspectos que contextualizam

a segurança e suas imperfeições no quesito humano e como objetivos específicos: apontar algumas falhas e suas conseqüências na prática da rotina social.

2. RECURSOS HUMANOS: ALICERCE OU VULNERABILIDADE?

A palavra credibilidade tem resumido o anseio das empresas quando o assunto é o reconhecimento do seu produto e da satisfação de seus clientes. Dependendo desse grau de confiabilidade criamos mecanismos que definem os laços dessa parceria. Seja no patamar das instituições ou ético moral social que perpassa por todo esse processo.

Com a revolução industrial o homem teve que se readequar a nova realidade de sociedade e tudo que veio pelo impacto capitalista se resumiu aos bens de consumo e suas conseqüências para a economia. Conseqüentemente a fomentação dos vícios de mercado acabou por si só criando um *Frankstein urbano* fadado a concorrência e as necessidades no desenvolvimento dos nichos industriais. Por sua vez à disputa pelo poder de mercado consumidor fez com que as informações se tornassem algo com peso de ouro, isso logo após a 2ª guerra mundial e a guerra fria entre os Estados Unidos da América e a antiga União Soviética.

Todavia toda estrutura em sua organização por mais que seja criteriosa e rígida, carrega em sua base o fator humano, condicionada a atos e decisões de grupos. O ponto fraco de toda essa pirâmide está na base, no alicerce desse sistema viciado que é o próprio ser humano. É ele que define as boas e más diretrizes que constitui os pilares de sustentação dessa cadeia informacional. Assim o nosso maior aliado pode ser o maior inimigo. Inclusive ao que diz respeito a uma famosa frase: “uma corrente é tão resistente quanto seu elo mais fraco”.

A maior vulnerabilidade de uma rede mora na insatisfação atrelada a uma ganância incontida. Com esses requisitos alguém pode destruir em questão de segundos todo um projeto rente aos planos de uma empresa para com um produto outrora guardado a sete chaves.

Independente do caráter daquela pessoa que traz a marca e a responsabilidade em um determinado grupo, uma das maneiras de evitar surpresas desagradáveis em um núcleo fechado de trabalho, é a valorização e reconhecimento desse componente, extraindo aquilo que ele tem de melhor para oferecer. Mostrar para ele o resultado real de suas atividades e os

desdobramentos que seu trabalho repercutiu dentro dessa organização. Tudo isso é uma fórmula básica para o sucesso de qualquer empresa e conseguinte, a segurança de suas informações. Portanto, segundo Meylan, citado por Prescott (2011), um funcionário que tem metas inatingíveis, trabalha em uma estrutura de opressão, não se sente confortável, não tem perspectivas de desenvolvimento na carreira, isso tudo cria um ambiente propício para se criar um ato ilegal.

Nesta perspectiva, ser seletivo na contratação de um funcionário requer buscar um profissional que compactue desde já com a filosofia da empresa. Nesse ponto crucial a companhia que necessita ter esse perfil de profissional em seus quadros, precisa inicialmente definir os rumos que se pretende tomar, pois o processo de segurança interna também depende desse fator.

Buscar formas de integração do funcionário a sistemática proposta por uma empresa contribui de certa maneira. Sejam através de programa de engajamento, eventos que requer extrair o lado mais humano, treinamentos que possam motivar as aptidões de cada um e demonstrar que esse empregado faz a diferença na empresa. Fomentando essa satisfação fará o funcionário a ter mais amor e respeito às normas da companhia.

DeMarco e Lister (1990, *apud* LAUREANO, 2005), afirmam que os principais problemas de segurança da informação em uma empresa não são de natureza tecnológica, mas sim sociológica, enfatizando o aspecto humano como o elo mais fraco de um processo de segurança da informação.

Porém, torna-se oportuno lembrar que as vulnerabilidades humanas não se restringem aos níveis operacionais das organizações, como também dos mais altos níveis hierárquicos. Goodchild (2010) afirma que profissionais em posição de liderança tendem a se mostrar desatentos para questões de segurança o que segundo ele deve-se principalmente ao fato de que estes profissionais acreditam estarem acima das regras de segurança da organização que a tecnologia de informação resolve qualquer problema que por ventura possa ocorrer. Neste sentido tornam-se alvos fáceis de golpes de engenharia social online, comprometendo assim a segurança dos ativos informacionais sob seu domínio.

3. POLÍTICA INTERNA GESTORA É LEI

Cada empresa tem sua própria cartilha para demarcar suas condições de trabalho e isso é logo aplicado no dia-a-dia da organização. Assim se cria um suporte imediato de como a segurança da informação é controlada e definida por esse caminho.

Com a contribuição de novas tecnologias ficou mais rígido o controle de celulares, emails e pendrives nas empresas, pois isso na realidade atual é uma porta aberta para quem quer burlar o sistema de segurança.

Embora haja uma linha muito tênue que separa as necessidades de um grupo em manter sigilo empresarial, há também a questão de censura e certas restrições que se aplica aos empregados. Como por exemplo, ate que ponto câmaras de vigilância pode interferir no lado psicológico dessas pessoas ou como lidar com o sigilo dos emails e seu conteúdo. Estes são alguns dos questionamentos que se fazem necessários no contexto das organizações para que o plano de segurança das informações não interfira de forma negativa no trabalho de sua equipe de profissionais.

Por outro lado, o fluxo desordenado e ilimitado de informações provenientes das ações humanas diretas, em geral traz possíveis riscos a ambientes que lidam com informação sigilosa. Devido a isso, é essencial uma política que possa prever riscos e ações a serem implementadas para que as informações sejam protegidas adequadamente. (FERREIRA, 2008)

A política de segurança da informação é apontada na literatura como condição *sine qua non* para que as empresas protejam seus ativos informacionais de forma satisfatória. O referido documento tem papel fundamental enquanto

> [...] um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais. (DIAS, 2000)

Trata-se, portanto de um documento estratégico cuja elaboração deve dar-se como uma construção coletiva envolvendo vários setores da organização, em especial gestores e profissionais de TI e segurança. Ferreira (2008) reforça que tais documentos precisam ser revisados periodicamente de forma a promover sua atualização em consonância com as

mudanças ocorridas no ambiente organizacional.

Outro aspecto relevante relacionado as políticas de segurança é a necessidade de que haja um compromisso institucional em fazer cumprir o que determina o referido documento, o que pressupõe uma ampla divulgação no contexto organizacional bem como medidas educacionais de forma a treinar a equipe para que a mesma adote os procedimentos determinados na política. (FERREIRA, 2008; LAUREANO, 2005)

3.2. A RADIOGRAFIA DA ANÁLISE DE RISCO: base para a construção de políticas.

Sem a malha fina de uma análise de risco numa corporação não há menor condição de observar os pontos fracos dessa organização. Por ela se identifica as possíveis falhas e o que isso pode acarretar a curto e longo prazo.

Podemos classificar essa radiografia inicial como: reconhecimento, análise e classificação – sendo que o reconhecimento recolhe e agrega informações sobre o ativo, a análise possibilita identificar essa relação direta e a classificação aponta o tipo de ameaça e seu grau potencial.

A análise preliminar de riscos pode ser considerada uma prévia no desenvolvimento inicial de um novo sistema ou projeto. Podendo assim ser interpretada como uma análise inicial qualitativa. Portanto não é meramente uma técnica específica, mas uma forma mais precisa de protocolo, permitindo dessa forma rever em tempo hábil uma possível ameaça e sua melhor prevenção.

3.3. CLASSIFICAÇÕES DAS INFORMAÇÕES: elemento crucial para a Segurança da Informação (SI)

Tendo como base alguns fatores seguir um padrão sistemático é essencial no desenrolar que permeia o sigilo, tais como: revisar o que foi diagnosticado – consiste em comparar o que está sendo criado, com algum parâmetro falho do passado; revisar a missão do que se destina – estabelecendo limites de atuação e delimitar o sistema que a missão irá abranger: a que se destinam, quem ou o que envolve e como será desenvolvida; Determinar os riscos – elaborar uma série de riscos e suas possibilidades; Revisar meios de eliminação –

levantar meios passíveis de eliminação e controle de riscos, indicando às melhores opções compatíveis as exigências do sistema; Analisar possíveis danos – pesquisar uma maneira mais eficiente para restrição, para limitação dos danos causados pela perda de controle sobre o risco; Indicar o responsável direto que irá solucionar qualquer eventualidade.

Neste processo é fundamental que as impressas elaborem a classificação dos ativos de informação que precisam proteger. Isto porque projetos de segurança da informação demandam recursos financeiros e humanos de forma que proteger tudo e com o mesmo nível prioritário pode representar desperdícios na empresa e ainda onerar excessivamente o projeto. Laureano (2005) ilustra tal afirmação ao dizer que

> Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, 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. (LAUREANO, 2005)

Beal (2005) enfatiza que não existe uma classificação informacional padrão para as organizações, esta vai depender do perfil, missão e objetivos de cada organização, porém afirma que esta deverá basear-se em aspectos tais como: importância, prioridade, e nível de proteção no contexto organizacional.

4. O PAPEL DO VERDADEIRO PROFISSIONAL

Como podemos constatar em nossa pesquisa, os conceitos sobre a segurança da informação apontam diversas análises, dentre elas podemos citar Pemble (2004) que sugere que a segurança da informação deve ser definida em termos das atribuições do profissional que é responsável por ela. Sendo assim ele descreve três pontos de possíveis situações na atuação desses profissionais e suas conseqüências diante aos fatos:

• O ponto operacional, que aponta os impactos resultantes ao que se referem aos incidentes nessa organização e o modo como isso é digerido e sustentando no negócio;

• O ponto da reputação, direcionado ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário; e por último:

• O ponto financeiro, voltado aos custos quanto a uma possível eventualidade de algum incidente.

Em qualquer nicho informacional, também podemos mencionar o fator surpresa

fomentado pelos *hackers* e *crackers* em sua eterna luta entre o bem contra o mal. Todavia, segundo Arce (2003), vários tipos de ataques em redes produzem um resultado em nível semântico, ou seja, mudam o significado da informação. Conseqüentemente, a mudança nos acessos das redes e a manipulação de falsos endereços de servidores, são exemplos clássicos destas investidas. Contudo, os mecanismos de detecção e prevenção agem no nível sintático: elas buscam caracteres focando padrões suspeitos, como por exemplo, um simples software de antivírus. Esta distinção acarreta um descompasso claro entre a ameaça ao se deparar de frente com o profissional da segurança.

Diante as responsabilidades impostas ao profissional de segurança da informação, Arce (2003) sugere que os sistemas operacionais junto a seus usuários, seriam os mais vulneráveis a ataques - embora, essa cadeia organizacional requer atenção a todos os níveis de usuários e sistemas.

Outra preocupação que deve ser discutido pelos profissionais, sendo isso de extrema relevância, é o custo da segurança da informação. De acordo com Geer Jr, Hoo e Jaquith (2003) mostram a despesa relativa para as correções de possíveis falhas de segurança em softwares, em cada estágio do processo. E quanto mais tempo se perde com danos não detectados no inicio do processo, maior é o custo que se tem.

Por isso, é de suma importância o papel do profissional da área ter em mente sua importância e competência que exige cada situação iminente de riscos.

4.1. OUTRAS ABORDAGENS NO CAMPO TECNOLÓGICO

Outro papel destes profissionais no campo de segurança, traz à tona outras discussões sobre novos conceitos e suas implementações ao que se cabe a prática de todo esse processo. Dentre várias vertentes conceituais, abordada por muitos autores, Hitchings (1995) apresentava, já há mais de uma década, a necessidade de um conceito de segurança da informação no qual o aspecto do agente humano tivesse a devida relevância, tanto como agente como paciente de eventos de segurança (ataques, mais especificamente).

No âmbito tecnológico, sugestões como a de Stergiou, Leeson e Green (2004) de uma alternativa ao modelo da OSI, ou como a de Aljareh e Rossiter (2002) de um modelo de segurança colaborativo, têm sido apresentadas em contraposição ao modelo vigente.

4.2. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A literatura - inclusive a não especializada, diga-se - é rica em relatos de incidentes de segurança da informação. Decerto, na realidade nua e crua, para um público incauto, este é o ponto mais insalubre da segurança: ela é muito mais reconhecida por suas falhas e imperfeições do que pelos aspectos positivos.

Furnell, Chiliarchaki e Dowland (2001) trazem um elemento particularmente sensível para os profissionais de segurança da informação: o uso de ferramentas de segurança para perpetrar ataques.

Com a disseminação de soluções de código aberto, várias ferramentas inicialmente desenvolvidas para a detecção de vulnerabilidades em redes, por exemplo, são difundidas e distribuídas livremente, totalmente gratuitas por todo o mundo. Esta situação, por sinal, tem sido utilizada por opositores ao modelo de software de código aberto, mas com conseqüências presumivelmente limitadas.

Vale ressaltar que a mais recente estatística do Centro de Estudos e Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) indica incidentes no segundo trimestre de 2011 um pouco superior a 127 mil, o que corresponde a um aumento de 40% em relação ao trimestre anterior e de 287% em relação ao mesmo trimestre de 2010. Mantendo a tendência observada no primeiro trimestre de 2011.

Além disso, no Brasil os gastos são maiores do que a média mundial e o período que as empresas levam em caso de desastre, se equiparam a de outras nações. Esse prazo gira em torno de três a quatro horas.

“É um grande avanço, se compararmos ao cenário de um ano atrás”, ressalta Vicente Lima, gerente comercial da Symantec no Brasil. Outra boa notícia aponta investimentos destinados a programas de recuperação de desastres e prevenções baseadas em treinamentos de funcionários na área de segurança de software.

A preocupação é tanta, que os executivos atualmente estão mais envolvidos com esse processo, do que era observado no passado e parte dessa corrida resulta do avanço da padronização virtual nas empresas. A implantação dessa nova tecnologia mudou em 74% das organizações o enfoque dos planos de recuperação de desastres.

Os três itens mais importantes na hora de manter as informações da empresa em

segurança são: a elaboração de políticas de segurança e o gerenciamento de suporte adequados, seguido do nível de conscientização dos funcionários.

Essa política interna atribui os 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. Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir essas normas poderá ser então considerado um incidente de segurança.

Os incidentes de segurança devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede, bem como o grupo de segurança e abusos da rede em que o usuário está conectado, seja um provedor, empresa, universidade etc.

5. SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS: O CASO FACEBOOK

O fato mais recente e discutido na mídia e quiçá, por aqueles que prezam a integridade que compete à segurança da informação, é o caso do Facebook, considerado hoje o maior site de relacionamento do planeta, difundido inicialmente por seu criador Mark Zucherberg.

Um breve histórico é essencial para a compreensão do citado caso, que exemplifica as fragilidades de um projeto em seu nível intelectual e prático, ao seu processo de segurança.

Independente do sucesso comercial do Facebook, Zucherberg enfrenta várias acusações de que sua criação foi fruto de idéias roubadas. Particularmente três estudantes de Harvard alegam que ele surrupiou suas idéias depois que o contrataram para programar um site de rede social que eles estavam criando.

O processo inicial se deu no momento que Zucherberg foi cconvidado para construir um site que pudesse ser compartilhado apenas no âmbito da universidade, com acesso para aqueles que tinham vínculo direto! Sendo assim, os estudantes poderiam postar fotos de si mesmos, colocar informações pessoais e pesquisar links.

Como ponta pé inicial o site se chamaria Havard Connection e teria como protótipo

duas seções: Encontros e Contatos. E de acordo com os envolvidos que se consideram lesados por Mark Zucherberg, os três rapazes – sendo dois deles irmãos gêmeos – alegam que ofereceram uma parte da companhia para ele, no instante que Mark concordou em trabalhar no site! Entretanto, depois de meses absorvendo a essência do projeto alheio, ele resolveu dispensar os antigos companheiros e decidiu lançar sozinho o que ele veio chamar de Facebook.(HOFFMAN, Claire. **Rolling Stones,** n.50, p.106 – 111, Nov. 2010.)

Controvérsias e especulações à parte, o sucesso do Facebook não foi instantâneo. Embora haja provas e evidências suficientes pela Justiça Americana que Mark tenha usado de má fé, e tomado para si algo que não era seu, ele conseguiu manter o sigilo de suas pretensões de maneira segura, longe do alcance de seus ex-companheiros de universidade.

Em contrapartida, nesse aspecto, manter um projeto em segredo do próprio programador, não é uma forma inteligente de garantir a segurança para quem dispõe de uma idéia no papel. Os três jovens que foram ludibriados aprenderam pelo viés mais difícil que o que requer a segurança de informações, não é apenas o fator sorte ou a escolha de pessoas por seu caráter, mas sim o fato de não ter registrado e averiguado o que cabe os direitos autorias de uma criação. Mesmo que para isso pudesse acarretar certo desconforto nas más intenções de alguém sem escrúpulos!

Por fim ao que cabe esse polêmico caso, independente do sucesso e dos fãs que usam e abusam do Facebook, a própria página já demonstrou falhas e fragilidades no quesito segurança também!

O Facebook é hoje o maior no ramo de rede social e é por isso que sofre ataques constantes, estando sujeito à vários tipos de *cyber crimes.*

Segundo um estudo da empresa de segurança Symantec, constatou que dois terços dos internautas de todo o mundo já foram vítimas de crimes digitais. A China lidera o ranking, seguido por Brasil e Índia, empatados com o segundo lugar. No Brasil um crime digital demora em média 43 dias para ser solucionado, levando a um prejuízo de US$ 1.408,09. (ALPHATECH BRASIL, 2010)

Outra pesquisa similar da Digital Society concluiu que a maioria das ameaças e quebras de segurança provém de redes sociais e o Facebook ganhou nota zero nesse quesito.

O vazamento de dados de usuários dos 10 principais aplicativos do Facebook para empresas de publicidade e de banco de dados ainda vai render dores de cabeça aos

administradores da rede social. Isso porque eles terão de expor ao congresso norte-americano mais detalhes do alcance do vazamento.

Os congressistas Edward Markey e Joe Barton enviaram uma carta a Mark Zuckerberg e demonstraram sua preocupação pelo fato de "aplicações de terceiros acumularem e transmitirem dados pessoais de usuários do Facebook". Por ter mais de 500 milhões de adeptos, "esta série de rachaduras na privacidade do consumidor é causa de grande preocupação".

Ainda na carta, os políticos pediram a Zuckerberg que especificasse o número de usuários afetados pelo vazamento, o momento exato no qual o Facebook tomou conhecimento do incidente e quais as atitudes seriam tomadas pela rede social.

O Facebook respondeu que estaria disposto a trabalhar com os congressistas para acabar com "qualquer confusão" gerada pelo vazamento, além de negar que o incidente possa se tornar um perigo para a privacidade dos usuários.

Um dos maiores problemas do Facebook são violações de senhas na própria página inicial do site, o username do usuário é usado como porta para esse tipo de crime. Há indícios de que programas desenvolvidos por *crackers* poderiam revelar a senha a partir do e-mail de login.

6. A FILOSOFIA PROTECIONISTA DE STEVE JOBS

Recentemente perdemos Steve Jobs, porém carregaremos seu legado através de suas criações revolucionárias do mundo da tecnologia. Suas invenções serão lembradas nos próximos anos e sua genialidade e empreendedorismo ímpar será sentido nas próximas gerações pelos desdobramentos de suas idéias sonhadoras.

Além de sua visão cosmopolita de mercado, Steve Jobs trazia em seu DNA uma percepção ampla da necessidade dos consumidores reais e potenciais. Sempre considerando que não havia limites para sua imaginação e que através dela, ele poderia facilitar e melhorar a vida das pessoas no mundo.

Jobs dominava como ninguém a arte de criar expectativas e isso o fazia o melhor de seu ramo. Trazendo em suas melhores intenções, um segredo guardado a sete chaves do que seria sua mais nova descoberta tecnológica.

Nenhum produto foi mais esperado com uma aura de mistério maior do que o IPhone, apresentado em janeiro de 2007. Segundo Jay Elliot, que escreveu o livro *The Steve Jobs Way*, a tática de reuniões de negócios para se discutir o IPhone, tinha como estratégia encontros rápidos, das quais participavam poucos engenheiros e pessoas da mais alta confiança de Steve. Um seleto grupo que tinha como missão compactuar com um projeto que mudaria para sempre os produtos eletrônicos.

Em suma, a Apple secretamente fez contato com empresas que a ajudaram no desenvolvimento da tecnologia de múltiplos toques no próprio visor de tela, o que antes era algo impensável nesse formato que propunha.

No dia da estréia do IPhone, ao som de Beatles e Bob Dylan, Jobs fez a platéia ovacionar sua mais nova invenção de uma maneira comovente. Arrancando espanto da imprensa e até mesmo da concorrência, que via tudo aquilo como algo inovador para nossa época.

O projeto do IPhone estava atrelado a cerca de 200 patentes, sendo todas elas contratadas na surdina de outras empresas. O que já demonstra a força e influência de Steve para a credibilidade e a formação sigilosa de mercado competitivo. (ALTMAN, Fábio.**Veja**, n.41, p.103, Out.2011)

Com uma eficácia impecável, Jobs mantinha fiel sua equipe e fazia de seus contatos uma extensão de sua confiabilidade que seu nome conseguiu angariar durante anos de trabalho, como gestor e visionário que ele assim o era. Criando desta forma, uma nova maneira de lidar com informações confidenciais sem usar de uma ditadura psicológica terrorista, diante aos seus funcionários e pessoas mais próximas, coniventes com seu trabalho para o bem de todos.

Hoje em dia, Steve Jobs é uma referência mundial não apenas pelas mudanças tecnológicas, como também alguém que desafiou os preceitos de mercado, sem vilipendiar a concorrência e/ou os segredos que ele trazia consigo mesmo. Independente da equipe que trabalhava com ele, sua filosofia de vida ficou impregnado na maneira protecionista empresarial, diante ao seu leque de produtos de ponta.

7. CONSIDERAÇÕES FINAIS

O desenvolvimento do estudo para realização do trabalho possibilitou conhecer diversos aspectos que compõem e norteiam a segurança da informação pela ótica humana e suas conseqüências.

O tema em foco discorreu sobre alguns pontos fundamentais que abordam essas falhas de conduta e o que pode ser melhorado, deixando evidente que para se chegar a algo mais seguro, necessita-se investir na capacitação do ser humano além de melhorias na metodologia das empresas. Demonstrando assim que valorizar o potencial do individuo e dá condições de trabalho e boas perspectivas, fará com que os índices que apontam tais fragilidades tenham um declínio mais evidente no que se resume a própria segurança dessas informações.

Conclui desta forma que, como nas demais áreas profissionais e do saber, a questão da segurança da informação junto ao elo mais frágil que se remete ao individuo, pode sim ter mecanismos precisos e mais confiáveis ao quer se refere à integridade de um grupo gestor.

REFERÊNCIAS

BEAL, Adriana. **Conceitos e Princípios Básicos da Informação**. In:_____Segurança da Informação. São Paulo: Atlas, 2005.

PRESCOTT, Roberta. **Fator humano: um dos pilares da segurança da informação.** Disponível em: **<** http://www.itweb.com.br/noticias/index.asp?cod=41990 **>.** Acesso 13 maio 2011.

MARCIANO, João Luiz Pereira. **Segurança da Informação: Uma Abordagem Social.** Disponível em:. **<** http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf >. Acesso 28 de agosto 2011.

SANTOS, Cleone Francisco; SILVA, Deverton Santana; GOUVÊA, João Paulo Hora. **Ameaças à Segurança da Informação: Os Riscos Humanos como Fator Prevenção.** Disponível em: < http://www.artigos.etc.br/ameacas-a-seguranca-da-informacao-os-riscos-humanos-como-fator-prevencao.html >**.** Acesso 14 maio 2011

GIARDINO, Andrea. **Incidente de segurança custa US$ 297,5 mil para organizações.** Disponível em:. < http://computerworld.uol.com.br/seguranca/2009/07/15/incidente-de-seguranca-no-pais-custa-us-297-5-mil-para-empresas/ > Acesso 12 de julho 2011.

ALTMAN, Fábio. As Idéias de Jobs para Mudar seu Mundo. **Veja**, São Paulo, n.41, p.103, Out.2011.

HOFFMAN, Claire. A Batalha do Facebook. **Rolling Stones,** São Paulo, n.50, p.106 – 111, Nov., 2010.