*Insider*s: Um Fator Ativo na Segurança da Informação

Gliner Dias Alencar[1], Anderson A. L. Queiroz[1], Ruy José G. Barretto de Queiroz[1]

[1] Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Av. Jornalista Anibal Fernandes, s/n – 50.740-560 – Recife – PE – Brazil

{gda2,aalq,ruy}@cin.ufpe.br

Abstract. *To achieve reliable levels of safety, the focus of many companies has been to invest primarily in technology and processes, forgetting the human resources that necessarily work with these technologies and will be part of the processes. Thinking about this gap, particularly in people as internal threats (insiders), the present study analyzed through theoretical and field research, aspects of information security at 34 public and private companies in Greater Recife where, in general, it was established that information security has a low level of maturity and active participation of insiders, these points that the paper proposes improvements.*

Resumo. *Para atingir níveis confiáveis de segurança, o foco de muitas empresas tem sido investir primariamente em tecnologia e processos, esquecendo-se dos recursos humanos que necessariamente trabalharão com estas tecnologias e farão parte dos processos. Pensando nesta lacuna existente, especificamente nas pessoas como ameaças internas (insiders), o presente trabalho analisou, por meio de estudos teóricos e pesquisa de campo, os aspectos de segurança da informação em 34 empresas públicas e privadas do Grande Recife onde, de uma forma geral, constatou-se que a segurança da informação tem um baixo nível de maturidade e existe uma participação ativa de insiders, pontos estes que o trabalho propõe melhorias.*

1. Introdução

Ao analisar a variável humana na Tecnologia da Informação e Comunicação (TIC), um dos pontos da tríade essencial (processos tecnologias e pessoas) para a efetividade da segurança da informação, segundo Gualberto *et al*. (2012), percebe-se que as pessoas podem se tornar uma ameaça à segurança da informação (SI) por diversos motivos e meios. Desde pessoas que facilitam a ação, sem nem mesmo saber que estão auxiliando o ato, àquelas que agem propositadamente e com finalidades específicas. Dentro do subgrupo de pessoas que agem de forma proposital, existem as que não têm ligação direta com o alvo do ataque, normalmente caracterizadas como hackers, e aquelas que têm algum tipo de conhecimento interno do alvo do ataque, os *insider*s, definidos como atuais, ex-empregados ou contratados (diretos ou indiretos) que têm ou tiveram acesso autorizado ao sistema e às redes da organização, assim como, conhecimento das políticas internas, procedimentos e tecnologia utilizada, empregando tais conhecimentos e privilégios como facilitadores para realizar ataques ou auxiliar invasores externos, sendo categorizados como uma ameaça interna.

A quantidade de pessoas envolvidas nos processos internos unida à falta de uma correta política de gerenciamento e manuseio das informações são aspectos que facilitam a ação dos *insider*s. Casos relacionados à perda de informações, roubos de

dados, engenharia social e sabotagem de TIC envolvendo *insider*s estão cada vez mais frequentes no noticiário nacional e internacional. Entre os exemplos relacionados a este tipo de notícia tem-se o caso do funcionário do setor de informática do *Bank of America* que foi processado pela justiça americana por ter instalado um software malicioso nos caixas eletrônicos do banco, o qual permitia que o empregado realizasse saques fraudulentos sem deixar nenhum registro, como descreve Rohr (2010). Segundo a Imperva (2009), um programador chinês que trabalhava na *Ellery Systems* nos EUA, transferia códigos fontes proprietários a uma empresa concorrente chinesa. A concorrência e a perda de códigos causaram a falência da *Ellery Systems*. Incidente parcialmente responsável pela criação da Lei de Espionagem Econômica em 1996.

Considerando que os fatos anteriormente mencionados são exemplos de situações frequentes no ambiente coorporativo, nota-se o quanto a variável pessoa pode ser danosa para a instituição, uma vez que a maioria dos incidentes, quer direta ou indiretamente, envolve a participação humana, gerando prejuízos muitas vezes incalculáveis, como ressalta Greitzer *et al.* (2008). Além da relevância social, é importante destacar a escassez de estudos que investiguem esta temática. Neste contexto, acredita-se ser relevante para a área de SI realizar estudos na tentativa de identificar as origens e comportamentos dos *insider*s e, também, verificar que atitudes as empresas adotam para lidar com tal ameaça.

Acredita-se também que a segurança deverá ser constituída em camadas, como cita Maccarthy (2010), dessa forma, qualquer melhoria implantada contribuirá para se ter um ambiente mais seguro. Com este pensamento, espera-se que o melhor entendimento das ameaças internas modifique o ambiente corporativo como um todo, provendo dificuldades para que as vulnerabilidades sejam exploradas, o que diminuirá os riscos e aumentará o patamar de segurança do ambiente, bem como se tem a expectativa que ações como a citada elevem o nível de maturidade da área de SI.

Visando compreender melhor e encontrar soluções para o problema exposto, foi realizada uma pesquisa com o intuito de analisar a visão técnica e estratégica da área de segurança da informação, especialmente os fatores relacionados às ameaças internas, nos ambientes corporativos de empresas com sede ou escritório na capital pernambucana, Recife, ou cidades circunvizinhas, tratadas no trabalho como "Grande Recife". Para tal, foi construído um questionário adequando, principalmente, o estudo de Gabbay (2003) realizado com empresas do Rio Grande do Norte, da pesquisa realizada pela Modulo (2006), com representação nacional, e da pesquisa realizada pelo Ecrime (2010), com entidades norte-americanas, assim como comparando-os.

2. Coleta e Tratamento dos Dados

Para a coleta dos dados foi utilizada a pesquisa de campo. Como características comuns utilizadas para delimitar a amostra utilizada, as empresas deveriam ter sede ou escritório no Grande Recife, com, no mínimo, quinze funcionários e ser da área de TIC ou ter uma área específica de TIC. O questionário utilizado foi composto por 43 questões divididas em seis categorias: Dados da Empresa, Dados do Respondente, Importância Estratégica da Informação, Ferramentas de SI na Empresa, Recursos Humanos e Estrutura Organizacional e, finalizando, Segurança da Informação Corporativa.

A aplicação do questionário foi proposta em 62 empresas, das quais 43 (69,4%) se propuseram a responder. Destas 43, nove questionários foram invalidados por não

responder completamente todas as questões não opcionais ou por conter respostas visivelmente incoerentes como, por exemplo, afirmar que tem atividade fim em TIC e ser do setor primário ou citar que não possui nenhuma política de segurança da informação e afirmar que a política é divulgada formalmente. Assim, a amostragem final é composta por 34 empresas distintas (54,8% das empresas propostas).

Todos os entrevistados eram funcionários das empresas, sendo que 31 deles (91,2%) eram responsáveis ou ligados à área que trata a SI e os demais 8,8% eram funcionários da TIC. A amostra é representada por 76% de empresas do setor terciário da economia e 24% do secundário, não tendo nenhuma empresa caracterizada no setor econômico primário, sendo 65% privadas, 26% públicas e 9% de economia mista. A quantidade de funcionários das empresas variou de 15 a 26 mil, enquanto a quantidade de computadores variou de 13 computadores a 8 mil máquinas, conforme Gráfico 1.

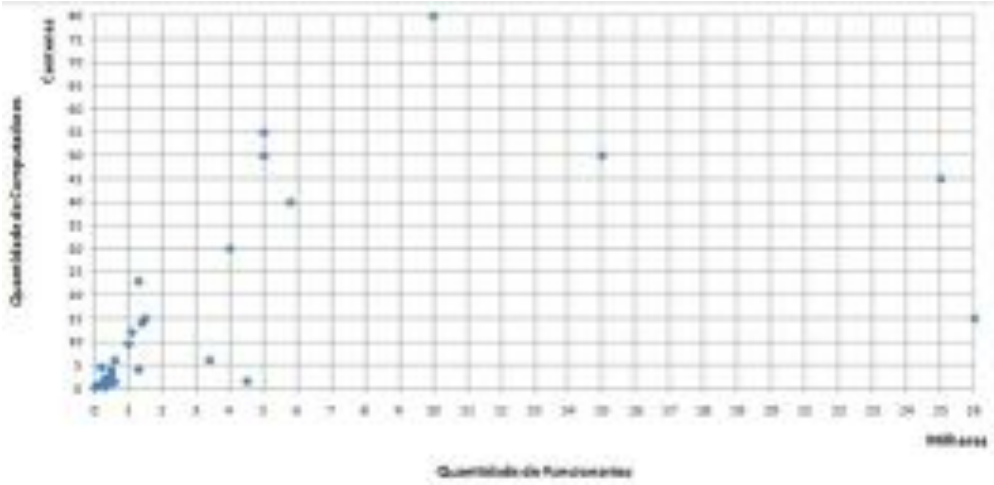

Gráfico 1. Amostra (quantidade de computadores x quantidade de funcionários)

Dentre as empresas pesquisadas, cinco empresas (14,7%) têm a TIC como área fim. A classificação quanto à área de abrangência foi de: 38% de abrangência nacional, 29% estadual, 18% regional, 9% multinacional e 6% local.

3. Análise Descritiva dos Resultados

3.1. Importância estratégica da informação

Foi visto que 91% das empresas acreditam ser muito importante as informações por elas guardadas ou manipuladas, enquanto 9% responderam como sendo importante (0% para as demais opções: nenhuma importância, pouca importância e neutra). No mesmo caminho, 76% acreditam que a perda ou vazamento das informações são muito prejudiciais para a corporação, enquanto 24% classificaram como prejudicial (0% para pouco prejudicial, não causa prejuízo e neutro). Corroborando com o conceito da era da informação colocado por Castell (2007), que aborda a informação como um bem vital.

Ao questionar se o assunto segurança da informação vem sendo debatido de forma sistemática e estratégica nas empresas nos últimos meses, 44% dos respondentes marcaram a alternativa ideal, o tema SI vem sendo tratado com a devida relevância. Porém, mesmo nos dias atuais, 9% das empresas afirmam que não estão tratando do referido tema nos últimos meses e nem se encontram preparados para discutir tal

assunto. Obteve-se, também, 38% respondendo que o tema é tratado, mas sem a devida relevância e 9% não debatem, mas deverá ser tratado em breve.

Ao questionar as empresas sobre a existência de divulgação institucional e frequente sobre a SI na corporação, 35% das empresas responderam de forma positiva e, em sentido contrário das boas práticas relativas à SI, grande parte das empresas (65%) registrou que não existe tal divulgação. Este número negativo tem uma representação ainda maior quando se questionou a existência de treinamentos periódicos ou processos de conscientização sobre SI para os funcionários. Nesta opção, 85% responderam negativamente, ou seja, que não existem treinamentos periódicos ou processos de conscientização sobre SI para os funcionários, enquanto 15% afirmaram a existência. Também indo contra os modelos ideais da área, a pesquisa verificou que apenas 21% das empresas pesquisadas têm o investimento em SI alinhado com os objetivos de negócio da empresa, o que seria a situação ideal; que a maioria (41%) respondeu que não estão alinhados e que 38% da amostra afirmam estar parcialmente alinhados. Este ponto também discrepou, mostrando um ambiente menos alinhado, dos dados da Modulo (2006) que mostrava que 33% estavam plenamente alinhados, 40% parcialmente, 16% pouco e 11% não estavam alinhados.

3.2. Ferramentas de SI na empresa

A pesquisa revelou que todas as empresas utilizavam antivírus e uma grande parcela (91%) utiliza, também, *firewall* para proteger seu ambiente, 76% utiliza controle *Web*, 65% controle de *email*, 41% IPS (*intrusion prevention system*) ou IDS (*Intrusion detection system*) e 12% outras ferramentas. Na mesma questão verificou-se que poucas empresas (32,3%) utilizam os cinco tipos de ferramentas mais comuns (antivírus, *firewall*, controle *web*, controle de *email,* IPS/IDS) e apenas metade das empresas pesquisadas utilizam as quatro ferramentas que podem ser consideradas básicas para a SI corporativa (antivírus, *firewall*, controle *web*, controle de *email*). Os itens desta questão, assim como de outras do questionário, extrapolam os 100% por ser possível a marcação de mais de uma resposta na mesma questão da pesquisa.

Ao questionar sobre as principais dificuldades para se implantar as ferramentas de SI na empresa, quatro itens se destacaram: restrições orçamentárias (47%), falta de priorização (41%), falta de conscientização dos funcionários (38%) e escassez de recursos humanos especializados (32%). Enquanto apenas 9% afirmaram não existir obstáculos. Um fato interessante é a divergência ao se analisar as empresas públicas e privadas separadamente. Nos órgãos públicos, as principais dificuldades registradas são escassez de recursos humanos especializados e falta de conscientização dos funcionários, ambos com 55% dos casos, e ninguém afirmou que não existia obstáculos. Já nas empresas privadas os mesmos itens receberam, respectivamente, 22,7% e 27,3%; destacando-se restrições orçamentárias (50%) e falta de priorização (40,9%).

3.3. Recursos humanos e estrutura organizacional

Analisando a organização setorial da SI e dos recursos humanos que tratam a mesma, a pesquisa revelou que em metade das empresas existe um setor ou equipe formal dedicada à SI. Neste ponto percebe-se uma melhoria dos dados mostrados pela Modulo (2006), que trazia 43% das companhias com um departamento de SI estruturado. Também foi visto que 50% das empresas contam com pessoas externas envolvidas

diretamente na área de SI, tais pessoas são oriundas de terceirização, contrato ou parcerias. Ponto esse que dobrou o percentual se comparado com as respostas da Modulo (2006) e que pode gerar sérios problemas como relata Cezar, Cavusoglu e Raghunathan (2010). Também se verificou-se que apenas 21% dos responsáveis pela SI trabalham exclusivamente na área.

A pesquisa retratou que 59% dos responsáveis pela SI tiveram capacitação ou formação relacionada aos conceitos gerais da área de SI (conceitos, políticas, normas, auditoria, criptografia, *malwares*) e 56% tiveram capacitação ou formação nas ferramentas de SI utilizadas na empresa. Percebeu-se também que 44% dos respondentes tiveram formação ou capacitação em ambas as áreas e 29% responderam que não tiveram capacitação ou formação em nenhuma delas. Fato esse que é corroborado pela pesquisa da Modulo (2006), apontando que 50% dos profissionais que lidam com SI nas empresas foram parcialmente capacitados, 18% plenamente, também 18% pouco capacitados e 14% não têm profissionais capacitados. Dados semelhantes também são exibidos por Gabbay (2003). Porém, percebe-se, no atual estudo, um aumento do percentual dos grupos totalmente capacitado e dos que não tiveram nenhuma formação.

Ao solicitar aos participantes que colocassem uma nota entre 0 e 10 para mensurar o conhecimento da equipe responsável pela segurança da informação, obteve-se uma média de 6,9 (mediana 7) para os conhecimentos gerais em SI e média 7,3 (mediana 7) para o conhecimento da equipe nas ferramentas de SI utilizadas. Finalizando a seção de recursos humanos do questionário, foi solicitado aos respondentes que marcassem todos os tipos de análises ou procedimentos utilizados e eliminatórios na seleção de colaboradores (funcionários, servidores, terceirizados, estagiários). Nesta etapa, viu-se o destaque para exame médico (85%), entrevista (71%) e análise de currículo e documentos (71%), porém percebeu-se um índice baixo das empresas que realizam uma avaliação da conduta ética e moral (12%) e, menor ainda, daquelas que realizam análise dos antecedentes criminais (9%) e exame psicotécnico (9%). Tais análises poderiam detectar possíveis comportamentos ou características que indiquem se o profissional tem ou não o perfil desejado, como aborda o Ecrime (2010) trazendo que 61% das empresas pesquisadas afirmam verificar os antecedentes dos empregados ou contratados como uma forma de segurança da informação.

3.4. Segurança da Informação Corporativa

A última seção do questionário, segurança da informação corporativa, iniciou-se questionando sobre o que se espera dos problemas e ameaças relativos à SI nos próximos meses. Com relação ao ambiente interno da empresa do respondente, 41% acreditam que deve aumentar os problemas e ameaças relativos à SI, 32% assinalaram que deveria permanecer os mesmo e 27% diminuir. Porém, ao fazer a mesma pergunta, agora abordando o ambiente externo (*Internet*), o número de respondentes que esperam o crescimento dos problemas e ameaças aumenta para 76%, enquanto 12% afirmaram que deveria permanecer os mesmos e, também, 12% que deveria diminuir. Tal expectativa de aumento, principalmente no ambiente externo, corrobora com os dados da Modulo (2006) e do Ecrime (2010), porém vai contra a pesquisa de Gabbay (2003), nele a maioria acreditava na diminuição dos problemas de SI. Também é visível a dissensão na expectativa relativa ao aumento de problemas de SI no ambiente interno e no ambiente global, o que corrobora com o pensamento de Schneier (2007) que aborda

a visão divergente das pessoas entre a segurança interna e externa, temendo, principalmente, o que é externo.

Ao questionar sobre as principais ameaças às informações nas empresas pesquisadas, os três itens mais votados estão diretamente ligados ao comportamento humano, sendo o primeiro e terceiro itens ligados, diretamente, ao comportamento das pessoas internas à empresa como pode ser visto no Gráfico 2. Tais informações locais dão uma visão diferente das demonstradas por Gabbay (2003), pela Modulo (2006) e pelo Ecrime (2010), o que mostra a dinamicidade da área de segurança da informação e as particularidades de cada ambiente.

Gráfico 2. Principais ameaças às informações na empresa

A SI corporativa pode ser entendida como a união de uma estratégia e de ferramentas específicas que atendam aos anseios corporativos para a implantação e manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança da informação (PSI) nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa. Alexandria (2009) corrobora afirmando, ainda, que a definição da PSI é o primeiro passo para o reconhecimento da importância da SI na organização e para seu tratamento adequado.

Sabendo da importância da PSI para o ambiente computacional das empresas, o questionário perguntou sobre sua implementação. Percebeu-se um resultado semelhante entre os que possuem uma PSI implementada e os que não têm (Sim, possui uma PSI formal implementada, 35%; Sim, possui uma PSI informal implementada, 15%; Não possui uma PSI implementada, mas está em processo de formulação ou implementação, 35%; e Não possui nenhuma PSI nem previsão de implementação, 15%). Fato bem diferente dos resultados de Gabbay (2003), quando 82% das empresas pesquisadas possuíam uma PSI implementada. Analisando apenas os órgãos públicos, 11% afirmou ter uma política formal implementada, enquanto 67% afirmou não possuir uma PSI implementada, mas está em processo de formulação ou implementação e 22% assinalaram não possuir nenhuma política de segurança nem previsão de implantação. Entre as empresas que já adotam uma PSI, 41% afirmaram que existe uma divulgação formal da política e é obrigado o seu conhecimento, sendo este o recomendado para a SI; enquanto 35% afirmaram que a PSI é disponibilizada para quem tiver interesse em conhecer, não sendo uma obrigação; e 24% citaram que não existia divulgação.

Os principais obstáculos citados pelos respondentes para que a PSI fosse implementada de forma eficiente foram a falta de priorização (76%), falta de conscientização dos funcionários (71%), escassez dos recursos humanos especializados (62%), restrições orçamentárias (59%) e falta de ferramentas adequadas (21%). Salienta-se que nenhum entrevistado citou que não existiam obstáculos. Tais respostas concordaram, em parte, com os resultados explanados por Gabbay (2003), nele as respostas que lideraram foram falta de conscientização dos funcionários (56%), falta de ferramentas adequadas (41%) e escassez de recursos humanos especializados (39%).

Algumas divergências nos resultados entre os setores público e privado foram observadas nesta questão, bem como ocorreu em outras. Para a área governamental, assim como observado na questão que aborda as dificuldades de implementação de ferramentas de SI, quem encabeça a lista, com 89%, é a escassez de recursos humanos, seguido pela falta de priorização (78%) e falta de conscientização dos funcionários (67%). Já nas empresas privadas, o principal obstáculo foi a falta de priorização (77%), seguido pelas restrições orçamentárias (64%). Ainda percebeu-se que, para 54% do setor privado, a escassez dos recursos humanos e a falta de conscientização dos funcionários são fatores de obstáculo.

Verificou-se também que, em 68% das empresas pesquisadas, não existe política de classificação e proteção às informações, fato que ocorreu em 100% das empresas públicas. Com relação à existência de níveis de controles ou políticas diferenciadas para acessar informações mais críticas, 47% da amostra afirmaram não haver. Neste ponto, mais uma vez, os órgãos governamentais destoaram, não existindo níveis de controles ou políticas diferenciadas para acessar informações mais críticas em 67% dos casos. Outro ponto levantado é que a ação de concordar, ao entrar na empresa, com algum tipo de termo de compromisso ou documento relativo à confidencialidade das senhas e informações internas ainda não é uma prática realmente difundida, sendo realizada por 50% da amostra ante 61% dos norte-americanos segundo o Ecrime (2010).

Ao requerer que selecionassem todos os métodos utilizados para segurança e controle de acesso aos meios tecnológicos e informações não públicas 100% das empresas assinalaram o uso do método de usuário e senha, mesmo resultado obtido por Gabbay (2003). Para melhorar o nível de segurança, 3% dos pesquisados afirmaram utilizar, também, certificado digital e outros 3% das empresas utilizam, além do usuário e senha, controle de acesso ao ambiente físico. Nenhuma empresa afirmou utilizar métodos mais avançados como biometria. Mesmo o usuário e senha sendo um método tecnologicamente superado, ainda é o mais comum nas empresas, como a pesquisa comprovou, corroborando o estudo de Shay *et al.* (2010), porém a sua administração ainda não segue as melhores práticas. Ao pesquisar sobre a existência de procedimentos para checagem de privilégios dos usuários de redes, assim como procedimento para bloquear a conta ou os privilégios imediatamente após não haver mais a necessidade, 32% afirmaram não existir tais recursos na sua empresa (sendo aumentado o valor para 67% ao analisar apenas os órgãos públicos), 12% marcaram a opção indeciso e 56% concordaram com a existência. Outro ponto é que 32% das empresas pesquisadas também responderam que não existe controles para obrigar os funcionários a trocar sua senha periodicamente, colocar senhas fortes e não repeti-las, novamente o valor dos órgãos públicos destoaram atingindo 67% para a opção citada. Nesta mesma questão, 65% dos entrevistados concordaram com a existência de tais mecanismos e 3%

assinalaram como indecisos. Já no panorama americano mostrado pelo Ecrime (2010) 80% das empresas afirmam utilizar uma política de gerenciamento de usuário e senha. Uma boa política de senha pode ser formulada sem grandes dificuldades e rapidamente terá um bom retorno no que tange à SI, conforme Shay *et al.* (2010).

Sabendo do valor que as informações têm no mercado atual, do aumento da capacidade de exploração de vulnerabilidades por parte dos atacantes e tendo como alvo o ambiente com vulnerabilidades, como a pesquisa vem demonstrando, é de se esperar que as empresas venham sofrendo ataques ao seu ambiente computacional. Fato que foi comprovado quando 47% das empresas afirmaram ter sofrido algum tipo de ataque visando os recursos tecnológicos ou informações nos últimos dois anos, 24% ficaram indecisos, não sabendo responder se realmente sofreram ou não tais tipos de ataques no período questionado, e 29% apontam que não receberam tais ataques. Números bastante semelhantes às respostas de Gabbay (2003), que retrata um ambiente que 45% sofreram ataques, 33% não sofreram e 21% não souberam responder.

Dentre as empresas que afirmaram ter sofrido algum tipo de ataque, 50% responderam que descobriram as vulnerabilidades exploradas, 29% não conseguiram detectar e 21% não souberam informar. Com relação à origem do ataque, 34% citaram que foi possível descobrir, 33% não descobriram e 33% não souberam informar. Continuando a considerar apenas as empresas que afirmaram ter sofrido algum tipo de ataque, 46% dos respondentes souberam informar a origem das pessoas envolvidas no ataque, sendo 21% de pessoas sem ligação direta com a empresa e 25% de *insiders*, ou seja, dos ataques em que foram descobertas as pessoas envolvidas, mais da metade (54%) eram *insiders,* e não atacantes externos como o senso comum normalmente aborda, fato corroborado por Schneier (2007).

Neste mesmo grupo, ao questionar sobre as perdas sofridas pelos ataques, 13% afirmaram, na opção outras do questionário, que não houve perdas. Todas as demais citaram algum tipo de perda, como: exposição de informações confidenciais (67%), perdas operacionais (58%), furto de informações sigilosas (38%), danos à reputação (38%), perdas financeiras (13%) e 8% para perdas de propriedade intelectual. Ordem diferente das empresas americanas citadas pelo Ecrime (2010) que traz a perda operacional como a mais citada, seguida por prejuízos financeiros e danos à reputação. Porém, mesmo sabendo quais as perdas, 75% citaram que não foi possível mensurá-las. Já na pesquisa da Modulo (2006) o número de companhias que não sabiam quantificar as perdas eram bem menor (33%).

Finalizando a pesquisa, foi possível perceber que todas as empresas têm medidas de segurança planejadas para os próximos 12 meses na corporação, o que demonstra, de certa forma, a ciência da situação. Entre as principais ações citadas como planejadas, percebe-se um foco mais macro para os projetos da SI corporativa (análise de vulnerabilidades com 47%, análise de risco no ambiente de TIC com 47%, adequação a normas, regulamentações ou legislação com 41%, política de segurança da informação com 32% e plano de continuidade de negócios com 26%) o que também foi demonstrado de forma semelhante na pesquisa da Modulo (2006).

4. Síntese da Análise

Ao aplicar os questionários e, consequentemente, analisar as empresas e os respondentes foi possível perceber, na maioria dos casos, que se tem conhecimento dos

problemas, dos métodos e tecnologias para melhorar o ambiente, bem como de que ações precisam ser feitas para que tais problemas sejam mitigados, contudo, não são realizadas as devidas ações e precauções necessárias, muitas vezes simples. O que corrobora com o estudo de Shay *et al*. (2010), pois o mesmo fala que os usuários normalmente se sentem mais seguros utilizando senhas fortes para *login*, mesmo assim costumam usar senhas fracas. Tal fato é percebido pelas respostas obtidas, onde, na maioria dos itens, não se teve assinalada a melhor alternativa, na visão da SI. Esta situação foi gerada, principalmente, por conta dos órgãos públicos, que demonstraram índices que, quando se diferenciava dos obtidos pela iniciativa privada, eram, em sua maioria, bem inferiores, o que também é citado na pesquisa da Modulo (2006).

A pesquisa relata que 44% das empresas têm o assunto segurança da informação sendo tratado com a devida relevância e se somar a este resultado a opção que ressalta que o tema SI vem sendo debatido de forma sistemática, porém sem a devida relevância, tem-se 82% das empresas. Contudo, não se vê sua aplicação prática, pois apenas 35% ressaltaram a existência da divulgação institucional da SI na empresa e em apenas 15% existem treinamentos periódicos ou processos de conscientização sobre SI para os funcionários. Outro indicador é que apenas 21% das empresas pesquisadas têm o investimento em SI alinhado com os objetivos de negócio. Foi possível perceber, também, que 100% das empresas trabalham com antivírus, contra 88% relatado por Gabbay (2003), e 91% com *firewall*s, mas estes bons números vão diminuindo para as demais ferramentas de SI. Outro ponto analisado, o percentual de empresas que utilizam procedimentos mais abrangentes para prover segurança como: controles ou políticas diferenciadas para acessar informações mais críticas, termo de compromisso ou documento relativo à confidencialidade das senhas e informações internas, PSI, procedimentos para checagem de privilégios e bloqueios de usuários de rede, obrigatoriedade de utilização de senhas fortes, sem repetição e com trocas periódicas, também não conseguiram atingir valores considerados satisfatórios.

Relacionado aos *insiders*, percebeu-se a participação ativa de tais ameaças em um ambiente com características que facilitam tais fatos, visto que as empresas pesquisadas não atentaram, ainda, para tal ameaça com o grau de importância que a mesma deve ter, ocorrendo falhas ou falta de procedimentos para a possível detecção dos *insiders* desde a sua contratação; bem como os procedimentos, metodologias e ferramentas internas, em sua maioria, não estão seguindo as melhores práticas, nem utilizando tecnologias mais avançadas de proteção. Inclusive atividades simples de capacitação, requisitos de senhas, políticas de permissões em estações, entre outras.

5. Estratégia para Mitigação das Ameaças Internas

Uma forma para o combate mais amplo e efetivo das ameaças, inclusive dos *insiders*, começa na identificação de todos os responsáveis por cada informação e verificar os direitos de acesso que cada pessoa ou perfil tem, tal trabalho se torna árduo pela quantidade crescente de dados armazenados e sistemas em produção. Após esse levantamento, é necessário, junto ao responsável da informação, verificar se os perfis concedidos ainda são necessários e estão de acordo com a política e regras atuais. Estabelecer ciclos de revisão de tais direitos ajuda a manter um ambiente mais seguro. Um processo de revisão dos direitos requer o estabelecimento de uma linha base para cada usuário, fornecendo informações aos proprietários dos direitos e aos responsáveis pelas aplicações ou dados, de forma que ambos estejam cientes da concessão e retirá-los

quando não forem mais necessários, como descreve Imperva (2010) de forma que os usuários possam trabalhar com o critério de privilégio mínimo, mas sem perder a usabilidade, com citam Motiee, Hawkey e Beznosov (2010). O ideal, segundo a Imperva (2010), é uma solução que integre atividades de monitoramento de arquivos, gerenciamento de privilégios de usuários e execução de políticas em tempo real.

Outro ponto possível para melhorar o combate às ameaças internas é a realização de exames com testes e análises que possibilitem a detecção de possíveis *insiders* na sua contratação e periodicamente em sua vida como funcionário, projetos de capacitação e incentivos à detecção de ameaças de forma automatizada e, também, pelos funcionários, provendo meios e incentivando para que as pessoas possam reportar tais fatos. Gerenciamento de mídias removíveis e dos acessos à *Internet* e *emails* também é um ponto a ser considerado. Porém, todas essas atividades devem ser regidas por uma PSI e normatizações mais efetivas e corretamente divulgadas, de forma que todos tenham ciência das regras e punições vigentes. Como citam Greitzer *et al*. (2008), os problemas relativos às ameaças internas estão cada vez mais em pauta, mas ainda tem muito que ser feito. No mínimo, o campo precisa de mais oficinas e cursos de formação para elevar a consciência dos gestores e dos profissionais da área de recursos humanos e TIC sobre os indicadores comportamentais e como diminuir os riscos. Nesta área a teoria dos jogos é um meio possível para auxílio no entendimento e na ajuda para definir estratégias organizacionais para mitigar tais ameaças, como ressalta, também, Moore, Clayton e Anderson (2009). Porém, é preciso reconhecer as potenciais consequências e questões éticas em torno de tais estratégias, pois podem gerar constrangimentos aos usuários, impactar negativamente a produtividade, afetar a moral dos funcionários e até ter consequências jurídicas.

Em suma, verifica-se a necessidade de uma estratégia formal para mitigação das ameaças internas. Tal estratégia deve englobar toda a trinca de segurança (tecnologia, processos e pessoas), ou seja, deve-se envolver a segurança física do ambiente e dispositivos, a utilização das ferramentas de segurança e monitoramento (antivírus, *firewall*, controle *web*, controle de *email,* IPS/IDS), segmentação da rede, definição de perfis para os usuários com os privilégios mínimos necessários; gestão dos incidentes ocorridos, corrigindo as vulnerabilidades para que não sejam exploradas novamente; PSI com suas normas e procedimentos; planos de capacitação, conscientização e marketing sobre segurança para que todas as pessoas envolvidas sejam educadas, conheçam os riscos, política e normas, e tenham ciência de como se precaver e tomar ações mais seguras; e, principalmente, com a utilização de meios de seleção mais abrangentes que envolvam análise social, comportamental e psíquica dos candidatos. Visto que uma análise mais apurada dos aspectos psíquicos e sociais podem detectar possíveis *insider*s, como retrata estudos específicos da área de saúde e humanas como as pesquisas de Baddeley (2010), Del-Ben (2005) e Flaxman (2010).

Para validar a proposta citada, dando uma visão mais holística da segurança da informação e questionando sobre dificuldades em sua aplicação, foi enviado um segundo questionário para 14 empresas da amostra inicial, sendo respondido por 9 delas (3 públicas e 6 privadas). Ao ser questionado se a estratégia citada conseguirá mitigar as ameaças internas, 89% das empresas responderam que sim. Uma empresa (11%) respondeu que não, afirmando que mesmo atacando todos os pontos da estratégia ainda é extremamente difícil combater as pessoas. Com relação às dificuldades na

implantação de um plano de segurança mais abrangente que envolva os pontos da estratégia colocada, os principais pontos citados foram: 44% afirmaram a dificuldade de integração das diversas áreas da empresa, também 44% alegaram problemas financeiros para implantação de medidas mais abrangentes, 33% citaram a capacitação das equipes para gerenciar o modelo como um todo, 11% afirmaram problemas com o apoio de tal modelo por parte do alto escalão da empresa e apenas 11% relataram não existir problemas. Tais resultados extrapolam 100% por ser uma questão aberta e existindo a possibilidade de citar mais de um problema.

6. Conclusões

Apesar da evolução das tecnologias, ferramentas e, principalmente, pesquisas na área de segurança da informação, não se observa a mesma evolução no meio corporativo, principalmente no que tange a área humana, como pode ser percebido ao comparar a pesquisa atual com pesquisas anteriores, como foi o caso de Gabbay (2003) e Modulo (2006). Também não se conseguiu, ainda, chegar aos bons níveis de maturidade reportados nas pesquisas norte-americanas, como os relatados no Ecrime (2010). Analisando pesquisas como a presente, é possível perceber que, na maioria das empresas, a segurança da informação tem um papel simplório, focado no tratamento de *malwares* e ataques externos, não realizando atividades simples para prover senhas mais fortes, rotinas de *backup* eficientes, implementação de ferramentas básicas de segurança, divulgação da SI, capacitação, entre outras. Tal situação faz com que não se consiga demonstrar seu real valor e obter recursos ou patrocínio para outros projetos na área. O que é comprovado quando se tem a restrição orçamentária como a principal dificuldade para a implantação de ferramentas de SI e a falta de priorização como principal obstáculo para implantação da PSI.

Desta forma, fica evidente a necessidade de evolução nesta área e da transferência da tecnologia para o meio corporativo visando uma estratégia que contemple os processos, tecnologias e, principalmente as pessoas em todas as suas fases, que inclui os aspectos psíquicos e sociais já abordados. Tal estratégia servirá não apenas para mitigar as ameaças internas, mas também como uma forma de se prover um ambiente mais seguro implementando a segurança de forma mais holística.

Referências

Alexandria, J. C. S. (2009) "Gestão da Segurança da Informação: Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica", Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo.

Baddeley, M. (2010). Herding, social influence and economic decision-making: socio-psychological and neuroscientific analyses. In: *Philosophical Transactions of The Royal Society*. Biological Sciences, 365, p. 281-290.

Castells, M. (2007), Era da Informação: A Sociedade em Rede, Editora Paz e Terra, Volume 1, 10ª Edição.

Cezar, A., Cavusoglu, H., Raghunathan, S. (2010). Outsourcing Information Security: Contracting Issues and Security Implications. In: *Workshop on the Economics of Information Security*, Harvard University, EUA.

Del-Ben, C. M. (2005). Neurobiologia do transtorno de personalidade anti-social. In: *Rev. psiquiatr. clín.*, v. 32, n. 1, p. 27-36.

Ecrime. (2010) "CyberSecurity Watch Survey: Cybercrime increasing faster than some company defenses", http://www.cert.org/archive/pdf/ecrimesummary10.pdf

Flaxman, E. (2010). The Cambridge Spies: Treason and Transformed Ego Ideals. In: *The Psychoanalytic Review*, v. 97, p. 607-631.

Gabbay, M. S. (2003) "Fatores Influenciadores da Implementação de Ações de Gestão de Segurança da Informação: um Estudo com Executivos e Gerentes de Tecnologia da Informação em Empresas do Rio Grande do Norte", Centro de Tecnologia, Universidade Federal do Rio Grande do Norte, Natal.

Greitzer, F. L.; Moore, A. P.; Cappelli, D. M.; Andrews, D. H.; Carroll, L. A.; Hull, T. D. (2008). Combating the *Insider* Cyber Threat. In*: IEEE Security & Privacy*, v. 6, n. 1, p. 61-64.

Gualberto, E. S., Sousa Jr, R. T., Deus, F. E. G., Duque, C. G. (2012). InfoSecRM: Uma Abordagem Ontológica para a Gestão de Riscos de Segurança da Informação. In: *VIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2012)*, p. 1-12, São Paulo.

Imperva. (2009) "The Anatomy of an *Insider*: Bad Guys Don't Always Wear Black", http://www.imperva.com/docs/ WP_Anatomy_of_an_*Insider*.pdf.

Imperva. (2010) "Five Signs Your File Data is at Risk", http://www.imperva.com/ docs/WP_Five_Signs_Your_File_Data_is_at_Risk.pdf.

Insider. (2010) "*Insider* Threat Research", http://www.cert.org/*insider*_threat/ more.html.

Maccarthy, M. (2010). Information Security Policy in the U.S. Retail Payments Industry. In: *Workshop on the Economics of Information Security*, Harvard University, EUA.

Modulo. (2006) "10ª Pesquisa Nacional de Segurança da Informação", http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf.

Moore, T.; Clayton, R.; Anderson, R. (2009). The Economics of Online Crime. In *Journal of Economic Perspectives*, v. 23, n. 3, p. 3-20.

Motiee, S.; Hawkey, K.; Beznosov, K. (2010). Do Windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices. In: *Symposium on Usable Privacy and Security*, Redmond, EUA

Rohr, A. (2010) "Funcionário do Bank of America instala virus em caixas eletrônicos", http://www.linhadefensiva.org/2010/04/funcionario-do-bank-of-america-instala-virus-em-caixas-eletronicos/.

Schneier, B. (2007) "BT Counterpane's founder and chief technology officer talks to SA Mathieson at Infosecurity Europe", http://www.schneier.com/news-040.html.

Shay, R.; Komanduri, S.; Kelley, G. K.; Leon, P. G.; Mazurek, M. L.; Bauer, L.; Christin, N.; Cranor, L. F. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. In: *Symposium on Usable Privacy and Security,* Redmond, EUA.