Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

v. 12, n. 3
set-dez 2013

Editorial

Foco nas organizações

Foco na tecnologia

Ensaios

Fast track SBSI

Nominata de avaliadores

ISSN: 1677-3071

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente, mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

INSIDERS: ANÁLISE E POSSIBILIDADES DE MITIGAÇÃO DE AMEAÇAS INTERNAS

INSIDERS: ANALYSIS AND POSSIBILITIES OF INTERNAL THREATS RISK MITIGATION

(artigo submetido em setembro de 2013)

Gliner Dias Alencar
Doutorando em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE) e Analista de Planejamento, Gestão e Infraestrutura em Informações Geográficas e Estatísticas do IBGE
gda2@cin.ufpe.br

Anderson Apolonio Lira Queiroz
Doutorando em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE) e Coordenador do Curso de Ciência da Computação na Faculdade dos Guararapes
aalq@cin.ufpe.br

Ruy José Guerra Barretto de Queiroz
Doutor em Computação pelo Imperial College of Science, Technology and Medicine e Professor Associado da Universidade Federal de Pernambuco (UFPE)
ruy@cin.ufpe.br

ABSTRACT

In our current globalized and highly competitive world, information is one of the most valuable organizational assets. In this context, information security has become a constant concern. 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 run processes. Those people could also become threats. Thinking about this gap, particularly focusing on people as an internal threat (insiders), this study investigated the current situation and trends in information security. By applying a questionnaire to public and private companies in Recife and the surrounding (called, in this study, Greater Recife), aspects of information security were analyzed, focusing on internal threats, where it was established that, in general, information security has a low level of maturity, is not aligned to the business, plays a simplistic role of only seeking protection against external threats. In this vulnerable environment, the active participation of internal threats was noticed. The situation is worse in the public sector. Finally, the work proposed actions to mitigate internal threats involving a broader view of information security, so that people are seen as another layer of security and not just a vulnerability.

Key-words: information security; human vulnerability; internal threats; insider; layered security; awareness and education of users.

RESUMO

No mundo atual, globalizado e altamente competitivo, a informação é um dos mais valiosos ativos das empresas. Nesse contexto, a segurança da informação tornou-se um motivo de preocupações constantes. 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 funcionar os processos. Pessoas essas que poderão, também, se tornar ameaças. Pensando nesta lacuna existente, especificamente nas pessoas como ameaças internas (*insiders*), o presente trabalho investigou o panorama atual e tendências para a segurança da informação. Analisou, por meio da aplicação de um questionário, os aspectos de segurança da informação, focando nas ameaças internas, de empresas públicas e privadas da cidade do Recife e circunvizinhança (denominada, no presente trabalho, Grande Recife) onde foi possível constatar que, de uma forma geral, a segurança da informação tem um baixo nível de maturidade, não está alinhada ao negócio, exerce um papel simplório com foco na proteção contra ameaças externas. Neste ambiente vulnerável, percebeu-se a participação ativa das ameaças internas, com situação ainda mais precária no setor público. Finalizando, o trabalho propôs ações para mitigar as ameaças internas envolvendo uma visão mais ampla da segurança da informação de forma que as pessoas sejam vistas como mais uma camada de segurança e não apenas uma vulnerabilidade.

Palavras-chave: segurança da informação; vulnerabilidades humanas; ameaças internas; segurança em camadas; conscientização e educação de usuários.

1 INTRODUÇÃO

Desde o início da indústria, pode-se citar a tecnologia como destaque na tentativa de aprimoramento dos processos operacionais, tendo seu marco principal na revolução da tecnologia da informação (TI), a partir da década de 70, com uma vasta quantidade de descobertas e com o advento do microcomputador e do microprocessador. Esta revolução propiciou uma série de avanços, nas mais diversas áreas, beneficiando os que detêm maior conhecimento a seu respeito (CASTELLS, 2007; NOBRE, 2009).

Na sociedade atual, competitiva e que necessita de ações e tomadas de decisões rápidas, a obtenção e a guarda do conhecimento é de suma importância. Neste contexto, a informação tornou-se um dos mais valiosos ativos das empresas, visto que as informações manuseadas nas corporações podem gerar tanto lucro como grandes prejuízos. Assim, o setor que gerencia a informação tornou-se estratégico nas organizações (CASTELLS, 2007; NOBRE, 2009).

Com o avanço da tecnologia, cada vez mais o conhecimento está sendo transferido da mente humana e dos papéis para os aparatos tecnológicos, cabendo à tecnologia da informação e comunicação (TIC) conduzir processos como a manipulação, a guarda e o tráfego de informações corporativas, muitas delas confidenciais, em diversos tipos de ambientes, podendo abranger ambientes heterogêneos, complexos e distribuídos.

Ao analisar a variável humana na TIC, um dos pontos da tríade essencial (processos, tecnologias e pessoas) para a efetividade da segurança da informação (SI), segundo Gualberto *et al*. (2012), percebe-se que as pessoas podem se tornar uma ameaça à segurança da informação 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: empregados que invadem sua própria organização (NAKAMURA; DE GEUS, 2007); ou mais amplamente pelo CERT Program[1] 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 para facilitar a realização de ataques ou auxiliar invasores externos (CERT, 2013), 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 informa-

[1] *CERT Program - Computer Emergency Readiness Team Program*. Universidade de Carnegie Mellon, EUA. http://www.cert.org

ções 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. Este incidente também é apontado como um dos pontos responsável pela criação da Lei de Espionagem Econômica, em 1996 (IMPERVA, 2009).

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 quer indiretamente, envolve a participação humana, gerando prejuízos muitas vezes incalculáveis, como ressaltam 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 segurança da informação 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 sugere 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 diminui os riscos e aumenta o patamar de segurança do ambiente, bem como proporciona a expectativa que ações como a citada elevem o nível de maturidade da área de SI, como avaliam Rigon e Westphall (2013).

Visando a 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, à pesquisa realizada pela Módulo (2006), com representação nacional, e a pesquisa realizada pelo Ecrime (2010), com entidades norte-americanas, além de compará-los.

2 PERSPECTIVAS HUMANAS NA SEGURANÇA DA INFORMAÇÃO

Não é de hoje que as pessoas, principalmente os usuários de computadores, são inseridas na lista das principais ameaças ou vulnerabilidades. Marciano e Marques (2006) defendem que o conceito de segurança da informação precisa ser abordado além dos processos e tecnologias, sendo necessária uma análise na ótica social, vislumbrando o comportamento humano, para que a segurança da informação (SI) atinja sua maior amplitude. Porém, mesmo estando listadas com uma vulnerabilidade, as pessoas estão envolvidas em todas as etapas da tecnologia, da concepção ao uso, passando pelo desenvolvimento e administração.

Diversos outros autores corroboram essa ideia (CASTELLS, 2007; ELLWANGER, 2009; NOBRE, 2009), afirmando que não há como garantir a segurança da informação em uma corporação investindo somente em equipamentos e recursos de tecnologia da informação (TI). No mesmo caminho, Marciano (2006, p. 139) afirma que "não se conhece qualquer solução meramente tecnológica para problemas sociais. Sendo um conceito eminentemente social, a segurança da informação necessita de uma visão igualmente embasada em conceitos sociais para sua correta cobertura". Schneier (2008) afirma que a segurança é tanto um sentimento como uma realidade, sendo necessário medir e analisar alguns aspectos reais, mas, também, analisar os aspectos psicológicos e ambientais do fato que nem sempre são concretos ou objetivos.

Uma explicação para este fato pode ser compreendida ao verificarmos que o assunto ainda não é totalmente consolidado na mente das pessoas, provocando medo ou fazendo com que o *cyberterrorismo* seja subestimado (SCHNEIER, 2007). Porém, aos poucos, a visão relativa às pessoas como integrantes da cadeia de segurança da informação está se alterando.

Abordando o assunto de segurança da informação de forma mais ampla e ressaltando, de forma superficial, os aspectos humanos, tem-se a norma NBR ISO/IEC 27002 (ABNT, 2005), atualmente em vigor, sendo uma tradução da norma internacional de Segurança da Informação - ISO/IEC 27002. A norma em questão iniciou sua publicação como ISO/IEC 17799, tendo sido homologada no Brasil em setembro de 2001 (ABNT, 2001), atualizada e, posteriormente, renomeada para ISO/IEC 27002 (ABNT, 2005). Um fato interessante nessa atualização é que, entre outras alterações, mudou sua compreensão do aspecto humano ao modificar sua antiga seção 6.2.1 "Educação e treinamento em segurança da informação", divulgada na primeira edição (ABNT, 2001), para a seção 8.2.2 "Conscientização, educação e treinamento em segurança da informação", divulgada na atualização da norma em 2005 (ABNT, 2005).

A literatura que trata das questões de ameaças e técnicas de segurança classifica as pessoas envolvidas em segurança de diversas maneiras. Existem nomenclaturas que designam os grupos de pessoas e suas funções, sendo eles: *Script kiddies, Cyberpunks, Black hat, White hat, Gray*

hat, Coders, Engenheiros sociais e *Insiders*. Nestes grupos pode haver sobreposições, ou seja, uma mesma pessoa pode ter características inerentes a mais de um grupo ou passar, em diversas etapas de sua vida, por vários grupos. Conhecer suas metodologias de ataques, como também suas verdadeiras funções, é essencial para melhor se proteger (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Os garotos dos *scripts* (*Script Kiddies*) são geralmente novatos na arte de explorar vulnerabilidades. Muito embora possam ser pessoas que tenham um bom conhecimento nos conceitos de programação, redes e sistemas operacionais. Tais garotos buscam *sites* que fornecem *scripts* prontos ou utilizam ferramentas prontas de ataques, sem mesmo entenderem em profundidade os códigos e metodologias em execução. Apesar disso, seus ataques podem ser bastante prejudiciais a empresas que tenham nível baixo de segurança. Normalmente esse é o início comum para a maioria dos membros dos demais grupos de especialistas em SI (*Cyberpunks, Black hat, White hat, Gray hat, Coders* e Engenheiros sociais). Quando os garotos continuam na "carreira", acabam se incorporando a um dos outros grupos, de acordo com seus ideais (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Cyberpunks têm profundo conhecimento do que estão fazendo. Normalmente, buscam descobrir vulnerabilidades em sistemas e aplicativos, por pura diversão ou *hobby,* e liberam essas informações na *Internet* ou até mesmo para as empresas responsáveis. Na maioria das vezes não têm intenções maléficas, mas, às vezes, as vulnerabilidades descobertas pelos *cyberpunks* caem em mãos erradas, gerando grandes prejuízos (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Os chapéus pretos (*black hat*) têm como principais objetivos roubar informações confidenciais das organizações com o intuito de vendê-las para as próprias empresas ou para outras empresas ou pessoas interessadas. Tem por objetivo, normalmente, fazer alguma chantagem financeira ou galgar vantagens competitivas no mercado. Normalmente tais ações têm apenas o cunho financeiro como motivação para o *black hat* (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Os chapéus brancos (*white hat*) normalmente são pessoas com alto conhecimento técnico e vasta experiência em SI que utilizam tal bagagem para realizar serviços de segurança como, por exemplo, reconhecer os pontos frágeis e vulneráveis em um determinado ambiente e aplicar ou sugerir correções. Porém alguns profissionais se apresentam como *white hat,* mas agem como *black hat*. Tais pessoas são categorizadas como *gray hat* (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Os *Coders* podem ser entendidos como um subgrupo dos *white hat.* Sendo profissionais que já tiveram uma experiência no mundo "maléfico" dos *hackers*, por exemplo, sendo *black hat,* e, posteriormente, usam essas experiências para escrever materiais de segurança (artigos, manuais ou livros) ou atuar como professores e consultores em palestras, seminários e

cursos. Um exemplo de *Coder* é Kevin Mitnick[2] (NAKAMURA; DE GEUS, 2007; RAMOS, 2007).

Outro agente comum na atualidade é o engenheiro social. Pode ser entendido como um *hacker* que utiliza mais as fragilidades do ambiente e humanas do que as tecnologias. Ou seja, é um profissional que desenvolve a habilidade de conseguir informações confidenciais por meio da persuasão ou manipulação de outras pessoas (NAKAMURA; DE GEUS, 2007; RAMOS, 2007). Segundo Alexandria (2009, p. 57), a "engenharia social ocorre quando alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso não autorizado a computadores ou informações sigilosas".

Os *insiders*, embora já tenham sido descritos brevemente na introdução, por representarem um ponto central do presente trabalho, serão abordados mais profundamente a seguir.

2.1 INSIDERS

Com as tendências de digitalização e compartilhamento de informações, os riscos associados aos *insiders* (sabotagem, fraude e roubo de dados sensíveis) têm aumentado, assim como os caminhos para o lucro a partir da venda de informações confidenciais. Neste ambiente, nem todos os *insiders* trabalham para si próprios. O crime organizado, os concorrentes e os países que desejam espionar descobriram que não há nenhuma razão para *hackear* por fora quando você pode recrutar pessoas de dentro, tendo um retorno do "investimento" muito maior quando se usa pessoas que já tenham confiança na casa. Os *insiders* normalmente são motivados pelo anseio financeiro, por vingança contra seu empregador ou pessoas ligadas a ele ou são forçados por meio de chantagens (IMPERVA, 2009).

Os *insiders* podem ser funcionários, ex-funcionários ou terceirizados. Como decorrência desse fato, torna-se extremamente difícil sua detecção, devido aos acessos oriundos de dentro das organizações, como também ao tempo disponível para verificar mesas, salas de equipamentos e até mesmo latas de lixo (RAMOS, 2007).

A Imperva (2009) ainda ressalta que existem *insiders* maliciosos e há *insiders* que são descuidados ou negligentes, o que altera o objetivo e responsabilidade em cada tipo. Porém, os danos resultantes podem ser os mesmos. O perfil dos *insiders* não segue o estereótipo dos *hackers* - socialmente desajeitados, sexo masculino, "viciados" por tecnologia desde a infância. *Insiders* também não são anônimos ou atacantes sem face, escondidos em um computador nos mais diversos lugares do mundo. Normalmente eles são funcionários comuns e, muitas vezes, acima de qualquer suspeita, podendo estar em qualquer empresa, pois, mesmo com um alto nível de recrutamento, não significa que um indivíduo com intenção maliciosa não seja contratado, ou que, ao longo do tempo, um

[2] Kevin Mitnick. http://mitnicksecurity.com/

doi:10.5329/RESI.2013.1203006

confiável e leal empregado não mude de lado, como mencionado nos exemplos abaixo, ocorridos nas agências de inteligência americanas (IMPERVA, 2009):

- Aldrich H. Ames – começou a trabalhar para a CIA[3] em 1962. Em parte devido à pressão de um divórcio e dificuldades financeiras, passou a espionar para a União Soviética, assim agindo por mais de duas décadas. Atualmente encontra-se cumprindo prisão perpétua, sem condicional.
- Robert P. Hansen - começou a trabalhar para o FBI[4] em 1976. Apenas três anos depois, em 1979, começou a espionar para os soviéticos e depois para os russos, sendo descoberto e preso apenas em 2001. Agora está cumprindo prisão perpétua, sem condicional.
- Ronald W. Pelton - começou a trabalhar para a NSA[5] em 1960 e se aposentou em 1980. Em 1984 começou a enfrentar dificuldades financeiras e vendeu segredos para a KGB[6] durante suas férias em Viena, Áustria. Pelton encontra-se cumprindo três sentenças de prisão perpétua consecutivas.

Segundo a pesquisa de Gelles (2012), muitos dos americanos presos por espionagem eram funcionários do próprio governo americano (*insiders*), sendo considerados confiáveis e leais quando foram analisados para iniciar a sua carreira profissional, mudando ao longo do tempo. O fato mais surpreendente é que a maioria daqueles que se tornaram espiões não foi seduzida, convencida, manipulada ou coagida a trair seu país, mas sim ofereceu seus serviços a um governo estrangeiro. Greitzer *et al*. (2008) também reforçam os números alarmantes dos casos de *insiders* no governo americano.

A motivação principal para a maioria dos *insiders* é dinheiro, seja por necessidade ou cobiça, mesmo que a quantia seja relativamente baixa. Há outros impulsionadores como atos de vingança, poder, política, medo, excitação e até aceitação social. Mas todas estas são menos importantes do que os objetivos financeiros citados por *insiders* capturados (IMPERVA, 2009).

Dentre os trabalhos mais relevantes na área de concentração do presente estudo está o *survey* americano (ECRIME, 2010) realizado pela CSO *Magazine*[7], CERT *Program,* Deloitte[8] e o *U.S. Secret Service*[9] apontando que os *insiders* são responsáveis por 26% dos eventos suspeitos

[3] *Central Intelligence Agency*. https://www.cia.gov/
[4] *The Federal Bureau of Investigation*. http://www.fbi.gov/
[5] *National Security Agency*. http://www.nsa.gov/
[6] *Komitet gosudarstvennoi bezopasnosti - State Committee for State Security*. Posteriormente sucedida pela FSB – *Federal Security Service of the Russian Federation*. http://www.fsb.ru/
[7] *CSO Magazine – Chief Security Officer Magazine – Security and Risk*. http://www.csoonline.com/magazine
[8] *Deloitte – Deloitte Touche Tohmatsu*. http://www.deloitte.com
[9] *U.S. Secret Service – United States Secret Service*. http://www.secretservice.gov

acontecidos nas corporações pesquisadas. O estudo também relata que 23% dos casos de acesso não autorizado ou uso de informações, sistemas ou redes; 11% das fraudes financeiras; 15% dos casos de roubo de informações; 11% dos casos intencionais de exposição de informações privadas ou sensíveis; 16% dos roubos de propriedade intelectual e 10% dos casos de sabotagem na TIC têm como origem os *insiders.* Corroborando os dados dessa pesquisa, tem-se o estudo realizado pelo Ponemon Institute[10] ressaltando que 88% das violações de dados foram causadas por negligência dos funcionários (SHIELS, 2009).

O relatório produzido pela Módulo[11] no Brasil (MODULO, 2006) ressalta que 33% das companhias não sabem quantificar as perdas e que 21% delas sequer conseguem identificar os responsáveis pelo problema. Segundo o mesmo estudo, quando as empresas conseguem identificar os responsáveis descobrem que a maioria das falhas de segurança que causam danos financeiros é originada por funcionários (24%), sendo seguidos por *hackers* (20%), problemas como vírus (15%), *spam* (10%) e fraudes (8%). Já nas indústrias, a mesma pesquisa mostra que a maior quantidade de problemas é relacionada com ex-funcionários (subgrupo dos *insiders*), o que representa 19% das citações.

Segundo Staff (2009) um terço dos trabalhadores roubaria dados para ajudar um amigo a arrumar um emprego, 39% dos pesquisados afirmaram que pegaria informações competitivas da empresa se constatasse que seu emprego está em risco e 48% admitiram que levariam as informações do trabalho consigo se fossem demitidos no outro dia. Dentre as informações roubadas, as mais desejadas são sobre clientes e detalhes de contratos, lemradas por 29% dos entrevistados. 18% disseram que visariam planos e propostas futuras, enquanto 11% citaram que levariam informações sobre produtos. Os resultados são corroborados pela informação que aproximadamente três quartos dos empregados roubariam segredos da empresa se fossem demitidos (RAYWOOD, 2010).

De acordo com as conclusões de Gabbay (2003), as ameaças existem nos ambientes interno e externo independentemente das medidas de segurança adotadas pela corporação e são igualmente prejudiciais para o negócio da empresa. Assim, é de suma importância o seu entendimento para que seja possível propor medidas de segurança voltadas a eliminar a causa do problema. Sullivan (2010) corrobora afirmando que apesar da maioria das violações que resultam na divulgação pública de dados de cartões de crédito nos Estados Unidos serem cometidas por pessoas externas, os *insiders* também são responsáveis por uma parcela significativa delas.

Especialistas em segurança afirmam que ataques gerados por *insiders* são cada vez mais comuns e muitos são evitáveis. Porém, nem sempre a contenção da vulnerabilidade ocorre, fazendo com que clientes

[10] *Ponemon Institute*. http://www.ponemon.org
[11] Módulo – Módulo Solutions for GRC. http://www.modulo.com.br

percam a confiança na empresa por ela não conseguir manter seus dados seguros (SHIELS, 2009). No mesmo documento, os especialistas ainda ressaltam que, embora os ataques internos sejam em menor número, eles podem ser mais devastadores, isso porque o funcionário sabe onde as "jóias da coroa" são mantidas. O roubo de informação ocorre desde pequenos arquivos até grandes blocos de dados, sendo geralmente motivados por vingança, medo ou ganância. Greitzer *et al.* (2008) e a Imperva (2009) complementam, citando que independentemente de se concentrar em sabotagem, fraude ou roubo de dados sensíveis, os *insiders*, normalmente, têm duas características que os beneficiam ante os atacantes externos: a confiança interna e o privilégio de acesso.

A perspectiva de ganho pessoal, profissional e financeiro pode conduzir a abusos, por parte dos *insiders*, dos seus direitos de acesso. Na maioria das organizações, os direitos de acesso do usuário aos dados e sistemas são muito superiores ao que é necessário para desempenhar suas funções. Isto ocorre porque os direitos são frequentemente concedidos, mas raramente revogados. Por exemplo, privilégios são concedidos aos usuários quando estão temporariamente em alguma função ou participando de algum projeto e não são revogados por quem os concedeu, ao final da atividade. Tampouco é comum o usuário solicitar tal remoção, quando suas necessidades mudam. Este excesso de permissão aumenta o risco de *insiders* maliciosos acessarem dados sensíveis (IMPERVA, 2010).

Executivos da Microsoft afirmam ser crescente a quantidade de ataques oriundos de *insiders* mal intencionados, sendo classificados como uma das principais ameaças às empresas e a maior preocupação no que se refere à segurança da informação. Considerando que o *insider* tem acesso, de forma relativamente fácil, aos ativos corporativos e os ataques podem ser de grande alcance, deve-se buscar no ambiente interno um equilíbrio entre as liberações visando à produtividade mas também à segurança (SHIELS, 2009).

Segundo a empresa de segurança McAfee, as perdas econômicas devido ao roubo de dados e violações de segurança geradas pelo crime organizado, *hackers* e *insiders* somaram US$ 1 trilhão em 2007. A Symantec[12], outra empresa de segurança, considera que a crise financeira pode conduzir a um aumento dos casos de violações gerados pelos *insiders* mal intencionados (SHIELS, 2009).

Schneier (2007) afirma que, de modo geral, existe na sociedade a preocupação com ameaças externas, enquanto as ameaças internas, advindas de pessoas próximas, são subestimadas. Por exemplo, nos Estados Unidos, a maioria dos sequestros é planejado por parentes da vítima; a maioria das fraudes de cartão de crédito é realizada por alguém que vive na mesma casa que o proprietário do cartão. Existe uma probabilidade maior de ser morto de forma violenta por algum conhecido

[12] Symantec Corporation. http://www.symantec.com

do que por um estranho. Entretanto, a grande maioria das pessoas teme o que é desconhecido, a ameaça externa. Com as corporações, não é diferente; as ameaças internas são subestimadas e deixadas em segundo plano.

2.2 PERSPECTIVA HUMANA PELOS VIESES SOCIAL E DE SAÚDE

Greitzer *et al.* (2008) afirmam que a ameaça interna se manifesta quando a pessoa sai do comportamento em conformidade com as políticas estabelecidas, independentemente dos resultados serem maliciosos ou um desrespeito às políticas de segurança. Para eles, os tipos de crimes e abuso de informação privilegiada associados aos *insiders* são significativos, envolvendo espionagem, sabotagem, terrorismo, extorsão, suborno e corrupção.

As ciências humanas e sociais não consideram os *insiders* normalmente como loucos, embora admitam que geralmente são emocionalmente perturbados ou sofrem de um ou mais transtornos de personalidade. Um transtorno de personalidade é reconhecido como um padrão de comportamento que é mal adaptado às circunstâncias em que ocorre, levando a conflitos nos relacionamentos, dificuldades no trabalho e mudanças emocionais periódicas (GELLES, 2012).

Nesta ótica, três pontos normalmente motivam esta alteração no comportamento dos *insiders.* Em primeiro lugar, a presença de uma fraqueza de caráter ou personalidade que se manifesta em tendências anti-sociais ou narcisismo, o que pode gerar comportamento execrável. Tendências anti-sociais podem ser percebidas quando os indivíduos rejeitam as regras sociais e normas ou quando pessoas não têm sentimentos de culpa ou remorso quando fazem algo errado. Em suma, faltam-lhes os valores que os inibem de tomar ações mal intencionadas ou realizar atos ilegais. Essas pessoas tendem a ser manipuladoras, egoístas e a procurar imediatamente gratificação ou retorno pelo que fazem. Finalmente, elas têm um apego limitado ou inexistente a coisas, lugares e pessoas, diminuindo assim sua capacidade de desenvolver um senso de lealdade (CONTOS, 2006; GELLES, 2012; IMPERVA, 2009).

Tais comportamentos anti-sociais também são tratados na área da medicina, quando os estudos apontam, inicialmente, que “além de fatores psicossociais, outros biológicos têm sido implicados na fisiopatogenia do transtorno de personalidade anti-social (TPAS). Estudos de neuroimagem apontam o envolvimento de estruturas cerebrais frontais, especialmente o córtex orbitofrontal[13], e a amígdala" (DEL-BEN, 2005, p. 27). O mesmo estudo ainda revela que “também tem sido sugerido que prejuízos na função serotonérgica[14] estariam associados à ocorrência de comportamento antisocial” (DEL-BEN, 2005, p. 27), visto que os pacientes com TPAS apresentam respostas hormonais atenuadas a estímulos farmacológicos. "O prejuízo da função serotonérgica tem sido implicado na etiolo-

[13] Córtex orbitofrontal: porção ventromedial do lobo frontal do cérebro.
[14] Sinapse serotonérgica: sinapse neurotransmissora específica.

gia de vários transtornos mentais, entre eles transtornos de ansiedade, depressão e transtornos relacionados ao controle do impulso" (DEL-BEN, 2005, p. 31). Essas características se correlacionam com os comportamentos mencionados pelos demais pesquisadores aqui citados e com os estudos de Baddeley (2010), para quem as alterações psicológicas e neurológicas são fatores para distúrbios sociais na área profissional e financeira.

O segundo ponto é a presença de uma crise financeira, pessoal ou profissional que expõe o indivíduo ao sofrimento e estresse extremo. O comportamento em relação a esse estresse é frequentemente observável no local de trabalho. Aqueles em posições de liderança devem ser treinados para identificar sinais de alerta precocemente (CONTOS, 2006; GELLES, 2012; IMPERVA, 2009).

O terceiro e último ponto é a ausência de assistência adequada em situações de crise. Outros podem deixar de reconhecer os problemas da pessoa ou podem reconhecê-los e se recusar a se envolver. A intervenção pode ser útil, mas se ninguém tenta ajudar, o indivíduo pode ter mudanças em seu comportamento que acarretem atividades maliciosas (CONTOS, 2006; GELLES, 2012; IMPERVA, 2009).

Entre os *insiders* analisados por Gelles (2012), não havia motivação única para espionagem. A verdadeira motivação foi sempre mais profunda do que aparentava (simplesmente pelo dinheiro, ideologia ou vingança). Por exemplo, os *insiders* analisados logo gastavam todo o dinheiro, sendo um fator aparente para sua posterior detecção. Também afirmaram que, mais importante do que se pode comprar, é o sucesso, poder e influência que o dinheiro simboliza, servindo como um bálsamo para as feridas de sua auto-estima em uma tentativa desesperada para atender às complexas necessidades emocionais. Outro fato interessante do mesmo estudo, e que segue a mesma linha, é que a maioria deles também informou que já realizou a espionagem simplesmente para contar aos amigos confiáveis sobre o que estavam fazendo, servindo como apoio emocional, como um esforço para impressionar ou para tentar envolver os demais na atividade.

Outro ponto que a maioria dos *insiders* tem em comum é a incapacidade de aceitar a responsabilidade por suas próprias ações, culpando sempre os outros pelos seus problemas, minimizando ou ignorando seus próprios erros ou falhas, sendo frequentes as falas de que roubar as informações foi muito fácil, pois a segurança física foi demasiadamente permissiva. Tal argumento remete a culpa à corporação por não fazer o suficiente para proteger as informações. Este sentimento comum ressalta que, provavelmente, nenhuma culpa sobre a traição foi sentida durante ou depois do fato, sendo considerado pelos autores dos incidentes apenas como uma transação comercial (GELLES, 2012).

Serafim (2003) corrobora tal pensamento afirmando que diversos aspectos comportamentais normalmente estão relacionados aos criminosos ou infratores, entre eles: loquacidade, superestima, mentira patológica, ausência de remorso ou culpa, insensibilidade afetivo-emocional,

estilo de vida parasitário, descontroles comportamentais, ausência de metas realistas a longo prazo, impulsividade, irresponsabilidade e fracasso em aceitar responsabilidade pelos próprios atos. Normalmente, os indivíduos apresentam grande parte dos aspectos supracitados simultaneamente.

Resultados semelhantes podem ser vistos nos estudos sobre casos de *insiders* relacionados à traição e espionagens realizados por Flaxman (2010), ressaltando o distúrbio de caráter dos *insiders*, sua ligação com frustrações de desejos no *Id*[15], distorções do *ego*[16] e defeitos no *super-ego*[17]. O autor ainda afirma que a traição não surge apenas pelo desenvolvimento da personalidade problemática individual, citando que a transformação psíquica do traidor normalmente tem pontos sociais e políticos atrelados ao seu desenvolvimento, bem como uma fonte psicodinâmica[18].

É fundamental entender, porém, que não é só porque um indivíduo tem ações ou aparenta comportamento anti-social ou narcisista, passa por uma grande crise, está em momentos de estresse extremo ou não recebe assistência adequada nas situações difíceis, que se torna uma ameaça interna. A maioria das pessoas tem, pelo menos, uma das fraquezas citadas em seu caráter ou personalidade ou passou por problemas como os citados. A pessoa como um todo deve ser avaliada e outras características positivas podem prevalecer sobre as negativas, o que na maioria dos casos ocorre (CONTOS, 2006; GELLES, 2012; IMPERVA, 2009).

Gelles (2012) ainda relata em sua pesquisa que as características positivas incluem a capacidade de aceitar críticas, de expressar a raiva e frustração de forma apropriada, ter autodisciplina, ter e cumprir metas a longo prazo, ser compassivo e atencioso em relação aos outros, capaz de cooperar e trabalhar em equipe para atingir objetivos comuns. É improvável que qualquer pessoa que possua estas características positivas em boa medida se envolva com esse tipo de traição.

Em resumo, o problema pode acontecer em qualquer lugar e com pessoas "inesperadas", por serem vistas como confiáveis e leais. Mas existem características comportamentais e de personalidade que podem servir de indícios para que sejam tomadas ações a fim de evitar que tais problemas fujam do controle. Serafim (2003, p. 75) ainda afirma que não necessariamente quem cometeu um delito cometerá outros, precisa-se "do exame criminológico acurado (investigação dos aspectos biopsicossociais do autor de um delito), diferenciando o criminoso ocasional do habitual". Tais exames e análises podem ser feitos para se selecionar profissionais, porém a eliminação de profissionais que têm características

[15] Id: conjunto psíquico que determina os desejos do sujeito.
[16] Ego: estrutura que aborda o conhecimento que o indivíduo possui de si mesmo e do meio.
[17] Superego: estrutura que relaciona os aspectos relacionados à moral e valores do indivíduo.
[18] Psicodinâmica: forças psicológicas que incidem sobre o comportamento humano, enfatizando a interação entre as motivações conscientes e subconscientes.

que os levam ao grupo de possível ameaça interna pode acarretar em dilemas, principalmente éticos e legais, pois, mesmo estando em um grupo mais propício, não se pode afirmar que a pessoa será um real infrator ou que um infrator terá esse perfil para sempre.

2.3 PERSPECTIVA HUMANA PELO VIÉS DO NEGÓCIO

Segundo Contos (2006), pela ótica da corporação, os *insiders* devem ser vistos como ameaças extremamente difíceis de serem controladas e podendo ter um grande conhecimento sobre o negócio, assim como acesso às informações mais sensíveis de maneira mais fácil do que aqueles que realizam o ataque por meios externos. Algumas formas de danos que as ameaças internas podem causar em uma perspectiva de negócios são: perda de dados confidenciais e de propriedade intelectual, redução da integridade dos dados, exposições de informações, destruição ou danos aos ativos críticos de informações, danos às comunicações empresariais e bloqueio de vendas ou de serviços prestados. Tais danos podem resultar diretamente na perda de clientes, diminuição da vantagem competitiva, perda da confiança dos acionistas e da credibilidade no mercado, danos à reputação e, de forma direta ou como resultado de tais perdas, prejuízos financeiros.

É evidente que nenhum destes resultados é positivo, mas uma organização deve ter ciência dos riscos e conduzir os negócios, não podendo simplesmente bloquear todos os seus dados em um cofre. A maioria das organizações não tem os recursos para proteger completamente todos os seus ativos (servidores, redes, *desktops*, dispositivos móveis, entre outros), mas deve se preocupar em garantir que a maioria dos sistemas de missão crítica, dados sensíveis e segmentos mais importantes de sua rede estejam em um ambiente com maior controle e garantias. Para chegar a este ponto, uma organização deve primeiro entender a sua postura de risco. Compreensão dos riscos é uma necessidade absoluta quando se tenta controlar ameaças à corporação, o que inclui os *insiders* (CONTOS, 2006).

A segurança é frequentemente avaliada em termos de risco, ou mais apropriadamente, do gerenciamento de riscos como ressaltam Rigon e Westphall (2013). A gestão de riscos é um processo metódico. Uma organização deve primeiramente identificar os ativos que ele está tentando proteger e mensurar o seu valor. Tais ativos podem ser tangíveis, tais como servidores, dispositivos de rede, informações de banco de dados e assim por diante. Por outro lado, podem não ter seu valor quantitativo realmente claro, sendo ativos intangíveis como a moral dos funcionários, a percepção do cliente, a fé dos acionistas e outras variáveis qualitativas para as quais é difícil atribuir um valor monetário (CONTOS, 2006).

Em seguida, a organização deve colocar em prática um mecanismo para gerenciar e controlar os acontecimentos negativos e compará-los com os custos. Simplificando, um equilíbrio deve ser alcançado entre o

custo de um incidente e os custos de prevenção, detecção e gestão de incidentes. Tal cálculo é comumente feito utilizando análises do retorno sobre o investimento e, especificamente nesse caso, do retorno sobre o investimento de segurança. Os cálculos e análises devem ser revisados, alterando os parâmetros utilizados de acordo com suas variações, que podem ocorrer por conta do próprio negócio, do mercado, alteração de prioridades organizacionais, assim como aplicação de novos métodos, tecnologias ou ferramentas de segurança (CONTOS, 2006). Rigon e Westphall (2013) detalham um modelo para aferição da maturidade da segurança corporativa.

2.4 PERSPECTIVA HUMANA PELO VIÉS TÉCNICO

Analisar e enfrentar as ameaças internas abordando uma perspectiva técnica incide em três áreas: prevenção de incidentes, detecção de incidentes e gestão de incidentes. As três soluções são extremamente importantes. Mas, individualmente, não têm a capacidade necessária para enfrentar as ameaças internas, devendo trabalhar de forma conjunta e ampliada (CONTOS, 2006; RIGON; WESTPHALL, 2013).

A prevenção, de uma forma completa, é considerada o padrão máximo em segurança. Se um *insider* simplesmente não tiver condições de fazer nada malicioso, o ambiente estará protegido contra ele. Do ponto de vista da tecnologia, isso é pleiteado, geralmente, por meio de produtos como *firewalls*, ferramentas de controle de acesso, sistemas de prevenção de intrusão (IPS), antivírus, encriptação de dados, concessão de acesso com privilégios mínimos necessários (MOTIEE; HAWKEY; BEZNOSOV, 2010), segregação de funções, autenticação forte (SHAY *et al.*, 2010), entre outros. Embora seja fácil ver projetos que pretendem implantar estratégias de prevenção, elas quase nunca são implantadas holisticamente para aumentar sua eficácia. Além disso, os meios de prevenções precisam de atualizações constantes, sendo caro e difícil de manter. Outro ponto é que, por conta dos problemas de interoperabilidade, não é oferecida uma maneira nativa para supervisionar toda a vasta arquitetura de um único ponto. Em suma, nem sempre o projeto tem condições para abranger todo o parque tecnológico (CONTOS, 2006).

Prevenção sem detecção de incidentes e gerenciamento de incidentes é como uma política de segurança da informação sem divulgação. Ela simplesmente não é suficiente para fazer todo o trabalho corretamente, pois, por mais que toda a prevenção seja tomada, informações devem ser utilizadas por pessoas ou sistemas que podem ser, justamente, a ameaça (CONTOS, 2006).

A detecção de incidentes trabalha, normalmente, no monitoramento das enormes quantidades de *logs* e alertas gerados a partir de dispositivos de rede, servidores, sistemas operacionais, aplicações, produtos de segurança, bem como dispositivos de segurança física e telefonia. Essencialmente, a detecção de incidentes está a procura de alguns grãos de areia maliciosos em um deserto de dados. Mesmo sendo uma tarefa árdua, a

maioria dos incidentes é descoberta por meio do monitoramento (CONTOS, 2006).

Uma vez que um incidente é identificado, as ferramentas e pessoas devem estar no local idealizado para que tal fato possa ser gerenciado, monitorado, medido, relatado e auditado. Assim, treinamento de funcionários, sensibilização para a segurança, políticas e procedimentos para a manipulação de um incidente são pontos que devem ser tratados corriqueiramente pela disciplina de gerenciamento de incidentes para que, no momento necessário, seja possível tomar as ações previstas. O gerenciamento de incidentes é a arma que une a detecção, prevenção, análise, políticas e procedimentos organizacionais. A resposta a incidentes, pelo gerenciamento de recursos para correção e fiscalização, permite que a organização seja eficiente e eficaz ao lidar com um incidente (CONTOS, 2006).

Percebe-se o desenvolvimento de pesquisas sobre o tema, *insiders*, nas mais diferentes áreas (técnica, negócio, social e saúde), mas usualmente de forma isolada. O que, para o tratamento do assunto no meio corporativo, pode ser ineficiente para garantir a segurança da informação. Tratando-se do assunto de forma combinada, o que demanda ações multidisciplinares, como se pretende no presente trabalho, que traz algumas áreas externas à computação, acredita-se poder obter melhores respostas para esse difícil problema.

3 METODOLOGIA

Quanto à forma de abordagem, a pesquisa desenvolvida pode ser considerada como quantitativa, pois os dados coletados foram traduzidos em números que, em seguida, foram classificados para que fossem realizadas análises baseadas em recursos e técnicas estatísticas (GIL, 2010; MARCONI; LAKATOS, 2010).

Do ponto de vista de seus objetivos, o presente estudo classifica-se, predominantemente, como uma pesquisa descritiva, uma vez que buscou descrever um fenômeno ou situação, mediante um estudo realizado em determinado espaço-tempo, sem a interferência ou manipulação do pesquisador e envolvendo o uso de técnicas padronizadas de coleta de dados tais como questionários aplicados no universo ou amostra (GIL, 2010; MARCONI; LAKATOS, 2010).

Para Gabbay (2003), Gil (2010) e Marconi e Lakatos (2010), as pesquisas científicas podem abranger um universo de elementos tão grande que se torna impossível considerá-lo em sua totalidade. Por essa razão, é frequente a utilização de amostras, ou seja, pequena parte dos elementos que compõe o universo. A amostra é, portanto, um subconjunto do universo, convenientemente selecionado, que deve ser o mais representativo possível do todo, para que resultados e características obtidos na porção estudada possam ser considerados como verdade para todo o escopo da população pesquisada.

Como características comuns utilizadas para delimitar a amostra utilizada na pesquisa, as empresas deveriam ter sede ou escritório no Grande Recife, com, no mínimo, quinze funcionários e ser da área de TIC ou ter, ao menos, uma área específica de TIC. O espaço geográfico do Grande Recife foi definido com objetivo de delimitar a área das empresas que seriam estudadas. A quantidade mínima de funcionários foi estabelecida por presumir que empresas com menos de quinze funcionários, em sua maioria, não teriam procedimentos ou preocupações formais com a segurança da informação. Tal motivo foi o mesmo para se impor a exigência de ser uma empresa da área de TIC ou ter departamento específico de TIC.

Para realização do estudo e coleta dos dados foi utilizada a pesquisa de campo. Segundo Gil (2010), Marconi e Lakatos (2010) e sendo corroborado por Gabbay (2003) e Nobre (2009), a pesquisa de campo é aquela utilizada com o objetivo de conseguir informações acerca de um problema para o qual se procura uma resposta pela interrogação direta dos sujeitos cujo comportamento ou característica se deseja conhecer. Ela consiste na observação de fatos e fenômenos tais como ocorrem espontaneamente na coleta de dados a eles referentes e no registro de variáveis que se presumem relevantes visando a fornecer os subsídios para uma correta análise e elaboração das conclusões.

Nesta pesquisa, o instrumento de coleta de dados foi um questionário, composto por 43 questões divididas em seis categorias, sendo elas: dados da empresa; dados do respondente; importância estratégica da informação; ferramentas de SI na empresa; recursos humanos e estrutura organizacional e segurança da informação corporativa.

Na construção do questionário alguns aspectos foram considerados, a fim de manter uma padronização nas questões apresentadas. Por exemplo, as questões que apresentaram alternativas de respostas, foram dispostas em ordem alfabética de modo a não induzir o respondente, com exceção dos casos em que há uma ordem crescente ou lógica das alternativas. Além disso, as opções abertas nas alternativas foram apresentadas por último, após as demais alternativas, apenas para efeito de padronização e diagramação do questionário.

A fase de análise de dados tem por objetivo interpretação e explicitação dos dados obtidos na pesquisa, organizando-os e sumarizando-os de tal forma que possibilite o fornecimento de indícios ou respostas ao problema proposto (GABBAY, 2003; GIL, 2010; MARCONI; LAKATOS, 2010). Para a análise e demonstração dos resultados, utilizou-se o modelo de estatística descritiva que, de acordo com Marconi e Lakatos (2010), consiste na tabulação dos dados por meio de frequência e percentagens das respostas obtidas e apresentação dos dados utilizando um conjunto de gráficos. Tais análises remetem à amostra citada, que, como em qualquer pesquisa estatística pode sofrer com características inerentes ao grupo abordado e não necessariamente do universo amostral como um todo.

Após a análise dos dados e levantamento dos pontos falhos, ou pontos de melhorias no ambiente, o estudo propõe ações de implantação ampla da segurança da informação para tratar os pontos levantados. Tais diretrizes compõem a estratégia para mitigação de ameaças internas e foram enviadas aos respondentes por *e-mail*, assim como um questionário como uma forma de validação prática da estratégia pretendida. Os dados deste segundo questionário foram novamente analisados por meio de estatística descritiva.

4 DA PESQUISA REALIZADA

A aplicação do questionário de pesquisa foi proposta em 62 empresas. Das empresas solicitadas, cinco ignoraram a solicitação (8%), quatorze alegaram não poder responder o questionário por conter informações confidenciais (22,6%) e 43 se propuseram a responder (69,4%).

Entre as empresas que responderam, nove questionários foram invalidados por não terem sido preenchidos completamente ou por conterem respostas visivelmente incoerentes como, por exemplo, afirmar que tinha atividade fim em TIC e ser do setor primário ou citar que não possui nenhuma política de segurança da informação, nem previsão de implementação e afirmar que a política é divulgada de maneira formal e é obrigação de todos conhecê-la. Desta forma, a amostragem ficou composta por 34 empresas distintas, o que representa 54,8% das empresas inicialmente previstas.

4.1 DADOS DAS EMPRESAS E RESPONDENTES

Para responder os questionários, procurou-se os responsáveis pela área de SI, quando a área existia, ou pela área que desempenhava as funções inerentes à segurança da informação. Todos os questionários foram respondidos por pessoas que trabalham no setor de TIC ou no setor responsável pela TIC da empresa, sendo que 31 deles (91,2%) são responsáveis ou ligados à área que trata a SI na empresa em questão.

A quantidade de funcionários das empresas pesquisadas variou de 15 a 26 mil, enquanto a quantidade de computadores variou de 13 computadores a 8 mil máquinas, conforme distribuição apresentada nos Gráficos 1 e 2, a seguir.

A amostra é representada por 76% de empresas do setor terciário da economia e 24% do secundário, não tendo nenhuma empresa caracterizada como sendo do setor econômico primário, sendo 65% privadas, 26% públicas e 9% de economia mista.

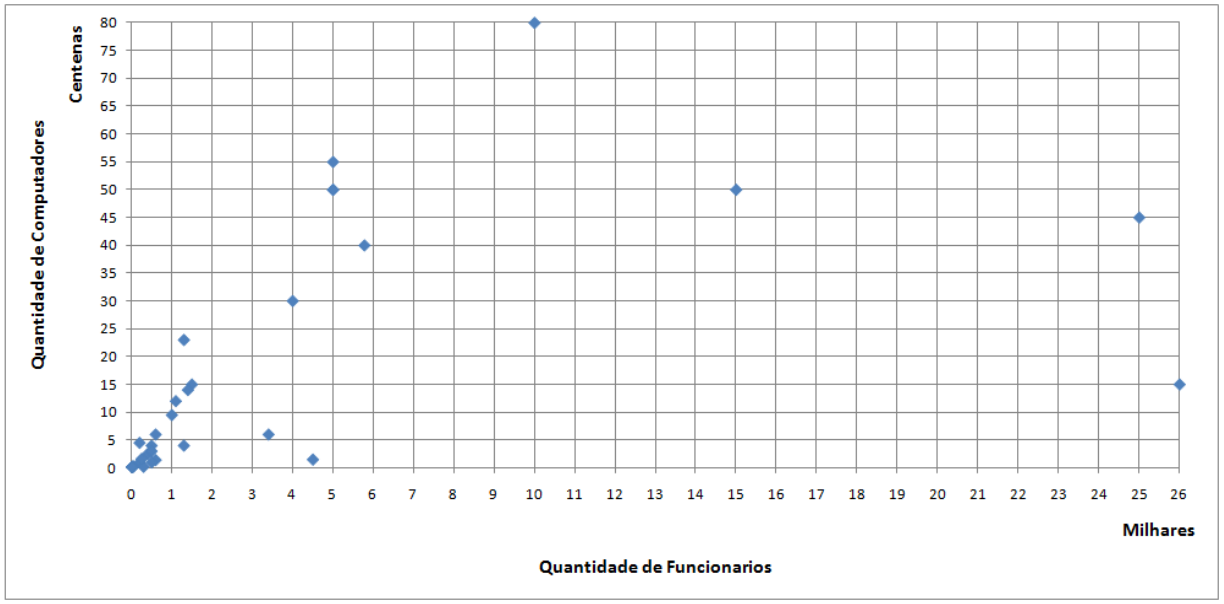

Gráfico 1. Dispersão da amostra

Fonte: elaborado pelos autores

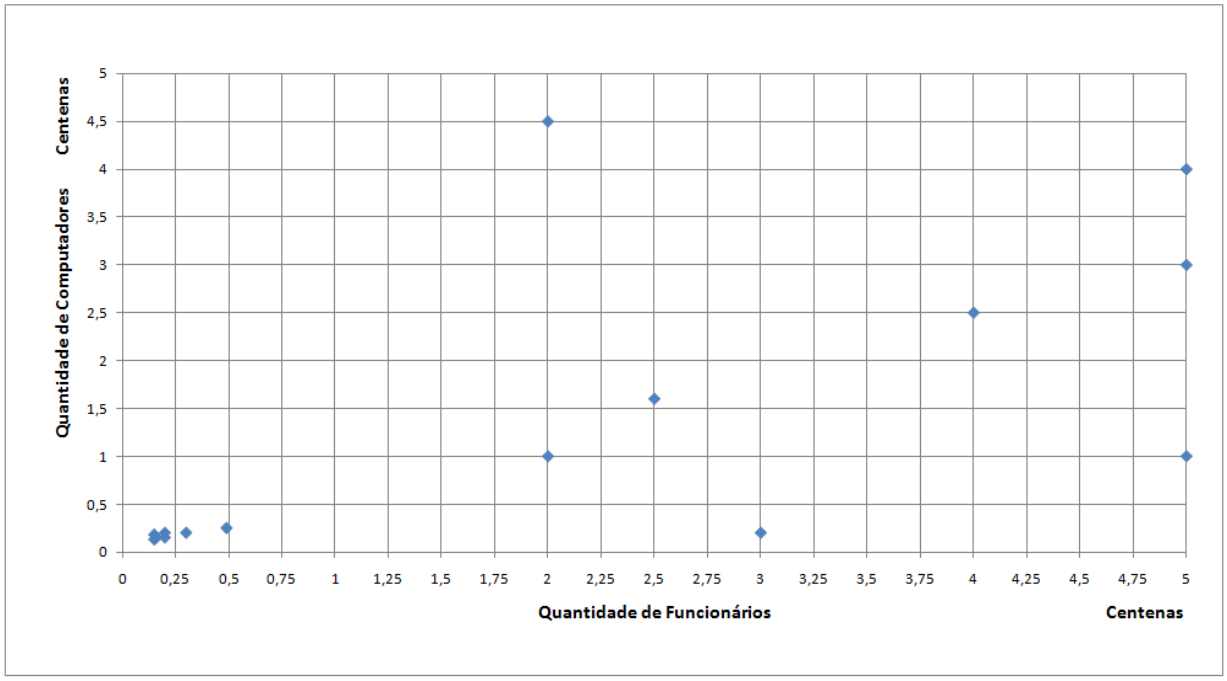

Gráfico 2. *Zoom* da área mais densa da dispersão da amostra

Fonte: elaborado pelos autores

Dentre as empresas pesquisadas, cinco empresas (14,7%) têm TIC como área fim. A classificação das empresas pesquisadas quanto a sua área de abrangência é demonstrada no Gráfico 3, sendo a maioria com abrangência nacional (38%), seguido pelas empresas com abrangência estadual (29%) e por aquelas que têm abrangência regional (18%).

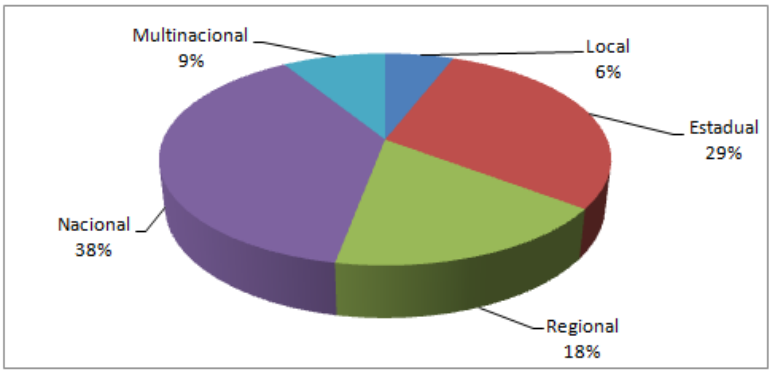

Gráfico 3. Abrangência das empresas pesquisadas

Fonte: elaborado pelos autores

4.2 IMPORTÂNCIA ESTRATÉGICA DA INFORMAÇÃO

A pesquisa demonstrou que 91% das empresas acreditam serem muito importantes as informações por elas guardadas ou manipuladas, enquanto 9% responderam como sendo importantes. Nenhum respondente considerou que as informações da empresa não têm nenhuma importância, são pouco importantes ou neutro. Apontando para o mesmo caminho, 76% acreditam que a perda ou vazamento de informações é muito prejudicial para a corporação, enquanto 24% classificaram como prejudicial, não havendo nenhuma resposta para as opções não causa prejuízo, pouco prejudicial ou neutro. Tais informações corroboram o pensamento de Castells (2007) e de Ramos (2007) no que tange à relevância das informações para as corporações na atual era da informação.

Ao questionar se o assunto segurança da informação vem sendo debatido de forma sistemática e estratégica nas empresas nos últimos meses, 44% dos respondentes consideram que o tema SI vem sendo tratado com a devida relevância, como pode ser visto no Gráfico 4. Porém, 9% afirmam que não estão tratando do referido tema nos últimos meses e nem se encontram preparados para discutir tal assunto.

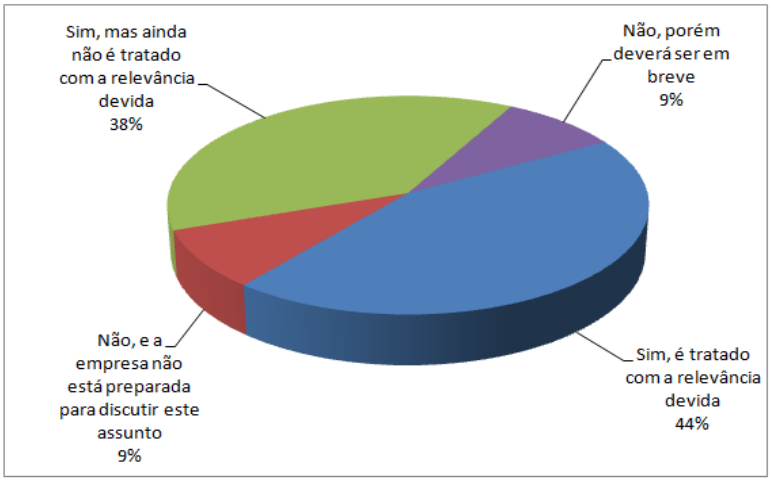

Gráfico 4. Relevância do assunto SI na corporação

Fonte: elaborado pelos autores

No trabalho de Gabbay (2003), 71% dos entrevistados afirmaram que o assunto SI vem sendo discutido de forma sistemática nos últimos meses, porém a pesquisa tinha apenas as opções: sim ou não. Considerando as respostas demonstradas no gráfico anterior apenas como sim ou não, têm-se 82% de respostas positivas, índice um pouco melhor que o obtido por Gabbay (2003).

Ao questionar as empresas sobre a existência de divulgação institucional e frequente sobre a segurança da informação na corporação, 35% das empresas responderam de forma positiva. Em sentido contrário das boas práticas relatadas nos capítulos anteriores, grande parte das empresas (65%) registrou que não existe divulgação institucional e frequente sobre SI na empresa. 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.

Também indo contra o que sugere a literatura que norteou este trabalho, a pesquisa verificou que apenas 21% das empresas pesquisadas têm o investimento em segurança da informação alinhado com os objetivos de negócio da empresa, o que seria a situação ideal; 41% responderam que não estão alinhados, conforme Gráfico 5. Este ponto também apresentou discrepância em relação ao esperado, mostrando um ambiente menos alinhado, se comparado as dados da Modulo (2006) onde 33% estavam plenamente alinhados, 40% parcialmente, 16% pouco e 11% não estavam alinhados.

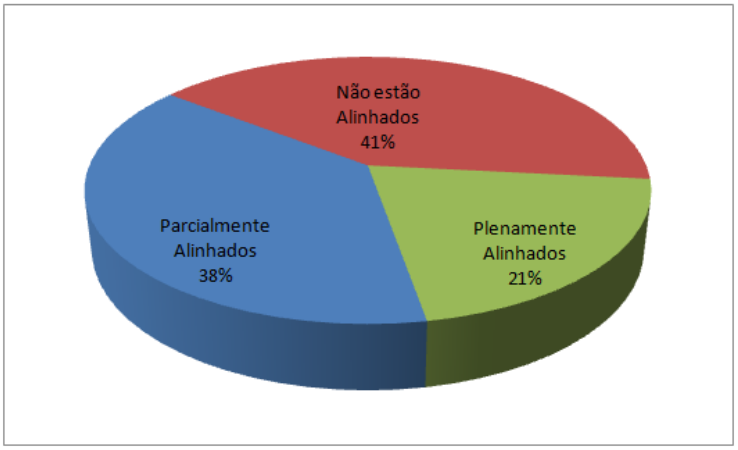

Gráfico 5. Alinhamento dos investimentos em SI com o negócio

Fonte: elaborado pelos autores

4.3 FERRAMENTAS DE SI NA EMPRESA

Com relação à utilização de ferramentas para segurança corporativa, a pesquisa revelou que todas as empresas utilizavam antivírus e uma grande parcela (91%) utiliza, também, *firewall* para proteger seu ambiente, conforme Gráfico 6. Na mesma questão verificou-se que poucas

empresas (32,3%) utilizam os cinco tipos de ferramentas mais comuns (antivírus, *firewall*, controle *web*, controle de *e-mail,* 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 *e-mail*). Os itens dos próximos dois gráficos (6 e 7), assim como os demais demonstrados em barra, extrapolam os 100% por ser possível a marcação de mais de uma resposta na mesma questão da pesquisa.

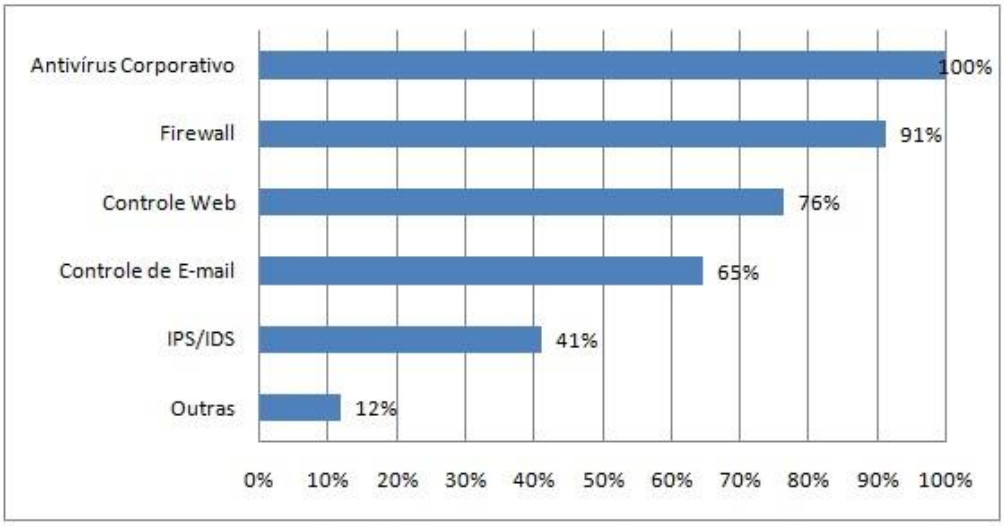

Gráfico 6. Utilização de ferramentas de segurança corporativa

Fonte: elaborado pelos autores

Ao serem questionados sobre as principais dificuldades para se implantar as ferramentas de segurança da informação na empresa destacou-se as restrições orçamentárias (47%) e a falta de priorização (41%). Apenas 9% dos entrevistados afirmaram não existir obstáculos, conforme Gráfico 7.

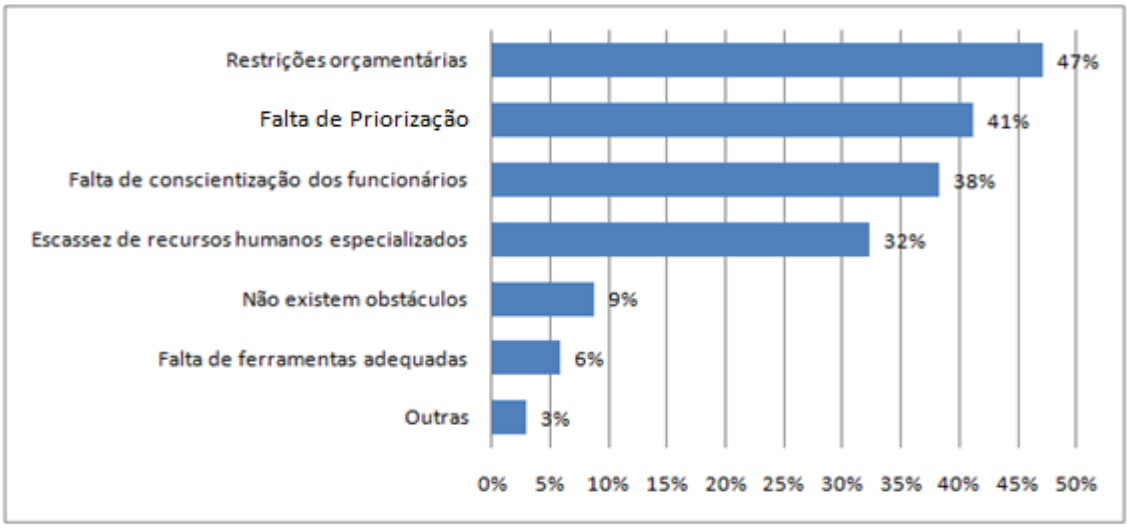

Gráfico 7. Principais dificuldades na implantação de ferramentas de SI

Fonte: elaborado pelos autores

Um fato interessante é a divergência ao se analisar as empresas públicas e privadas separadamente no que tange os dados do gráfico anterior. Nos órgãos públicos, as principais dificuldades registradas são escassez de recursos humanos especializados e falta de conscientização dos funcionários, ambos com 55% dos casos. Ninguém afirmou que não existia obstáculos. Já nas empresas privadas os mesmo itens receberam, respectivamente, 22,7% e 27,3%; destacando-se restrições orçamentárias (50%) e falta de priorização (40,9%).

4.4 RECURSOS HUMANOS E ESTRUTURA ORGANIZACIONAL

Analisando a organização setorial da segurança da informação e dos recursos humanos que tratam dela, a pesquisa revelou que em metade das empresas existe uma área, departamento, unidade ou equipe formal dedicada à segurança da informação. Neste ponto percebe-se uma melhoria dos dados mostrados pela Modulo (2006), onde 43% das companhias tinham um departamento de SI estruturado. Também foi visto que 50% das empresas contam com pessoas externas envolvidas diretamente na área de SI, em virtude de terceirização, contratos ou parcerias, percentual duas vezes maior ao previsto pela Modulo (2006) e que pode gerar sérios problemas como relatam Cezar, Cavusoglu e Raghunathan (2010).

Foi possível verificar que apenas 21% dos responsáveis pela segurança da informação trabalham exclusivamente na área. Sabendo que 50% das empresas alegaram ter um setor formal dedicado à SI, conforme parágrafo anterior, isso significa que menos da metade dos responsáveis por esse setor trabalha exclusivamente para prover a segurança da informação corporativa.

A pesquisa retratou que 59% dos responsáveis pela segurança da informação tiveram capacitação ou formação relacionada aos conceitos gerais da área de segurança da informação (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. Isto é corroborado pela pesquisa da Modulo (2006), na qual é apontado 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. Os dados exibidos por Gabbay (2003) também são nessa mesma linha. Porém, percebe-se, no atual estudo, um aumento do percentual dos extremos, grupo totalmente capacitado e dos que não tiveram nenhuma formação.

Ao solicitar aos participantes que atribuíssem uma nota entre 0 e 10 para mensurar o conhecimento dos responsáveis e envolvidos com implantação ou administração da segurança da informação, ou seja, a equipe de SI, mesmo que informal, 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.

Em um contexto geral, percebe-se uma média relativamente boa, em torno de 7, porém, ao analisar separadamente os grupos que afirmaram que os responsáveis pela segurança tiveram capacitação ou formação nas duas áreas em questão, a média sobe para 8,5 (mediana 8) nos conhecimentos gerais e média 8,7 (mediana 9) no conhecimento das ferramentas de SI utilizadas. Já o grupo que respondeu que os responsáveis pela SI não tiveram capacitação ou formação em nenhuma das áreas, a média diminui para 4,6 (mediana 5) para os conhecimentos gerais e, para o conhecimento nas ferramentas de SI, média 5,3 (mediana 5).

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 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%), conforme Gráfico 8.

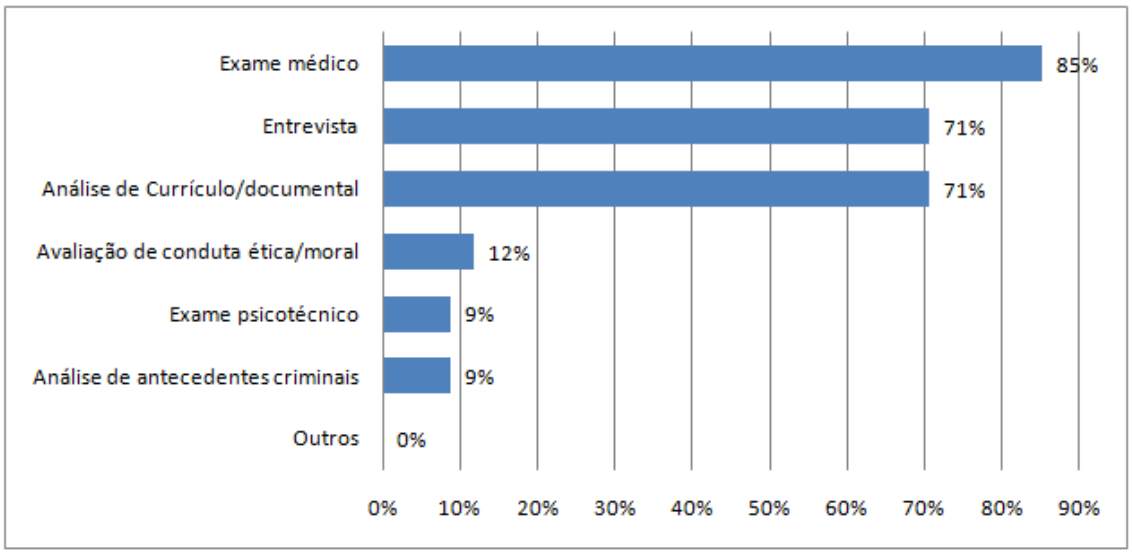

Gráfico 8. Análises e procedimentos utilizados na seleção de profissionais

Fonte: elaborado pelos autores

Tais análises poderiam ajudar a detectar possíveis comportamentos ou características que indiquem se o profissional tem ou não o perfil desejado. Para o Ecrime (2010), 61% das empresas afirmaram verificar os antecedentes dos empregados ou contratados como uma forma de garantir a segurança da informação.

4.5 SEGURANÇA DA INFORMAÇÃO CORPORATIVA

A última seção do questionário, segurança da informação corporativa, iniciou questionando sobre o que se espera dos problemas e ameaças relativos à segurança da informação nos próximos meses. Com relação ao ambiente interno da empresa do respondente, 41% acreditam que devem aumentar os problemas e ameaças relativos à segurança da informação (Gráfico 9). 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% (Gráfico 10).

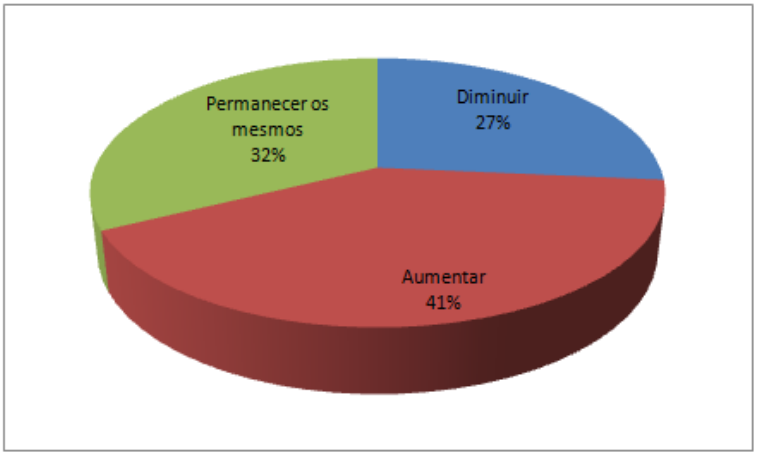

Gráfico 9. Expectativa dos problemas e ameaças à SI na empresa

Fonte: elaborado pelos autores

Tal expectativa de aumento, principalmente no ambiente externo, corrobora os dados da Modulo (2006) e do Ecrime (2010), porém vai contra as expectativas dos entrevistados por Gabbay (2003), que acreditavam na diminuição dos problemas de SI.

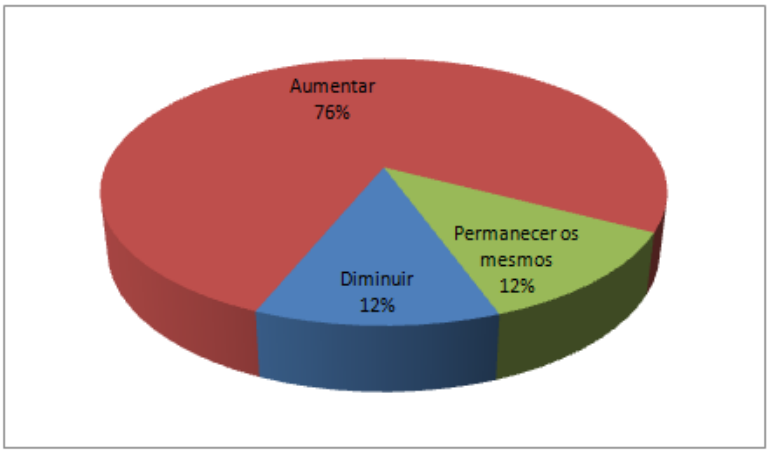

Gráfico 10. Expectativa dos problemas e ameaças à SI na *Internet*

Fonte: elaborado pelos autores

Também é visível a dissensão na expectativa relativa ao aumento de problemas de SI no ambiente interno e no ambiente global, o que corro-

bora 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 se questionar sobre as principais ameaças às informações nas empresas pesquisadas (Gráfico 11), os três itens mais destacados estão diretamente ligados ao comportamento humano: divulgação indevida de senhas (59%), acessos não autorizados (41%) e pessoas insatisfeitas ou sem capacitação (38%). Sendo o primeiro e terceiro itens ligados, diretamente, ao comportamento de *insiders*. Tais informações locais dão uma visão diferente da demonstrada pela Modulo (2006), por Gabbay (2003) e pelo Ecrime (2010), o que mostra a dinamicidade da área de segurança da informação e as particularidades de cada ambiente.

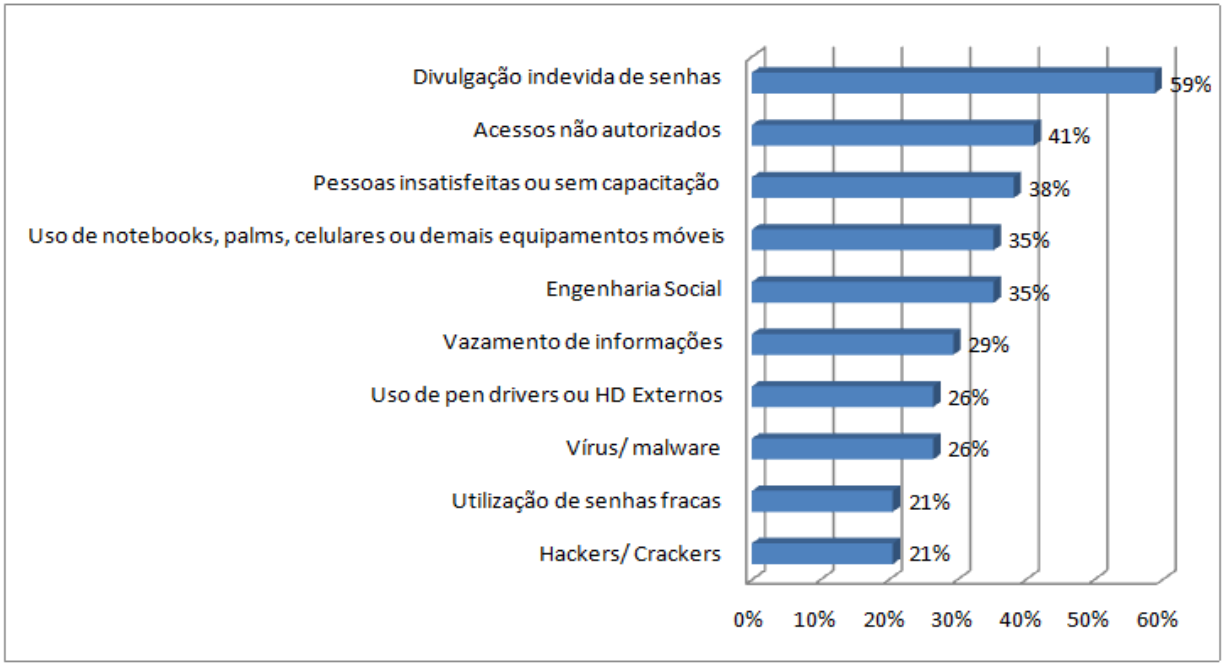

Gráfico 11. Principais ameaças às informações na empresa

Fonte: elaborado pelos autores

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 nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa. Para Alexandria (2009), a definição da política de segurança da informação é o primeiro passo para o reconhecimento da importância da SI para a organização e para seu tratamento adequado.

Sabendo da importância da política de segurança da informação 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 a têm, conforme pode ser visualizado no Gráfico 12. O resultado é bem diferente dos obtidos por

Gabbay (2003), para quem 82% das empresas pesquisadas possuíam uma PSI implementada.

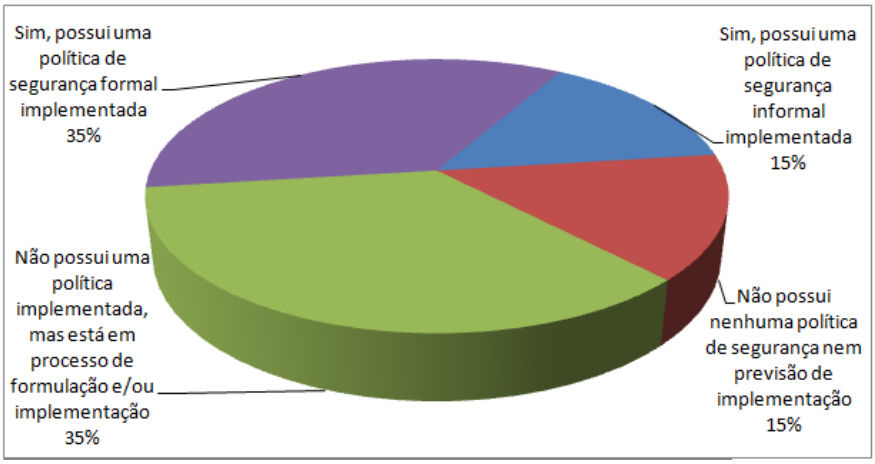

Gráfico 12. Estágio de implementação da PSI corporativa

Fonte: elaborado pelos autores

Analisando separadamente o grupo de órgãos públicos, apenas 11% afirmaram ter uma política formal implementada, enquanto 67% afirmaram não possuir uma política implementada, mas estar 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 conhecimento por parte dos funcionários (Gráfico 13), sendo este o melhor caso para a segurança da informação.

Entre os principais obstáculos citados pelos respondentes para que a política de segurança da informação seja implementada de forma eficiente estão a falta de priorização, com 76%, seguida pela falta de conscientização dos funcionários, com 71%, conforme Gráfico 14, o que corrobora, em parte, os resultados obtidos por Gabbay (2003), cujas respostas mais frequentes foram falta de conscientização dos funcionários (56%), falta de ferramentas adequadas (41%) e escassez de recursos humanos especializados (39%).

Assim como ocorreu em outras questões, houve uma divergência nos resultados entres os setores público e privado. Para a área governamental, semelhantemente ao que foi 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, seguida 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%), seguida das restrições orçamentárias (64%). Finalizando, 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.

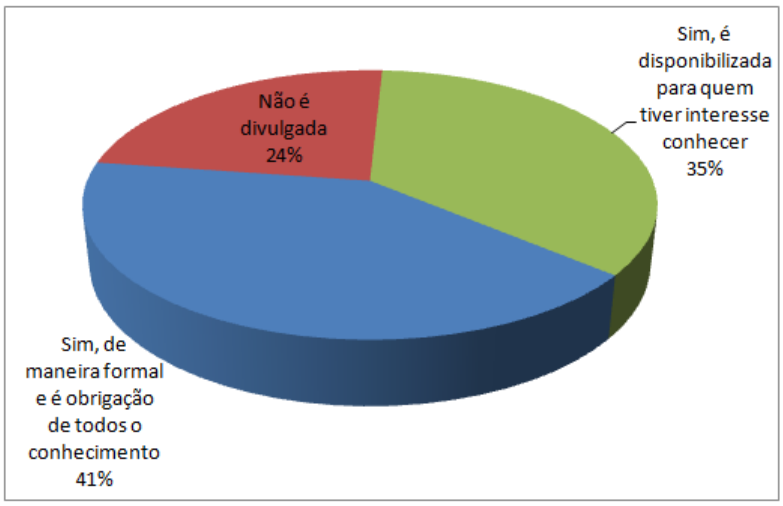

Gráfico 13. Divulgação da PSI corporativa

Fonte: elaborado pelos autores

A escassez de recursos humanos foi citada pelas empresas públicas como a principal dificuldade para se implementar a política e as ferramentas de SI. Em um contexto geral, esta foi a quarta dificuldade mais mencionada para se implantar as ferramentas de SI e a terceira na implementação da política, o que corrobora a percepção de dificuldades e desafios inerentes ao assunto do presente trabalho.

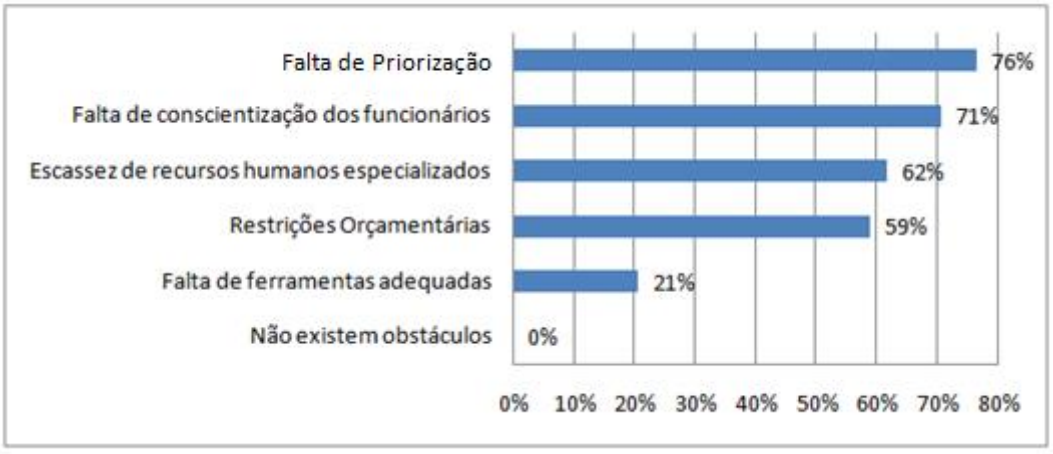

Gráfico 14 4.1. Principais obstáculos para implantação da PSI

Fonte: elaborado pelos autores

Verificou-se também que, em 68% das empresas pesquisadas, não existe política de classificação e proteção das 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 com algum tipo de termo de compromisso ou documento relativo à confidencialidade das senhas e informações internas, ao entrar na empresa, ainda não é uma prática realmente difundida, sendo realizada por 50% dos pesquisados ante 61% no mercado norte-americano (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, mesmo sendo um método tradicional e que vem sendo utilizado maciçamente por anos, a pesquisa verificou que a sua administração ainda não segue as melhores práticas.

Ao pesquisar sobre a existência de procedimentos para verificação 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 empresa (Gráfico 15), um percentual ainda maior (67%) se considerados os órgãos públicos, separadamente. 32% das empresas pesquisadas também responderam que não existirem controles para obrigar os funcionários a trocar sua senha periodicamente, colocar senhas fortes e não repeti-las (Gráfico 16). Novamente, os resultados para órgãos públicos foram piores, atingindo 67%. Já no panorama americano mostrado pelo Ecrime (2010), 80% das empresas afirmam utilizar uma política de gerenciamento de usuário e senha.

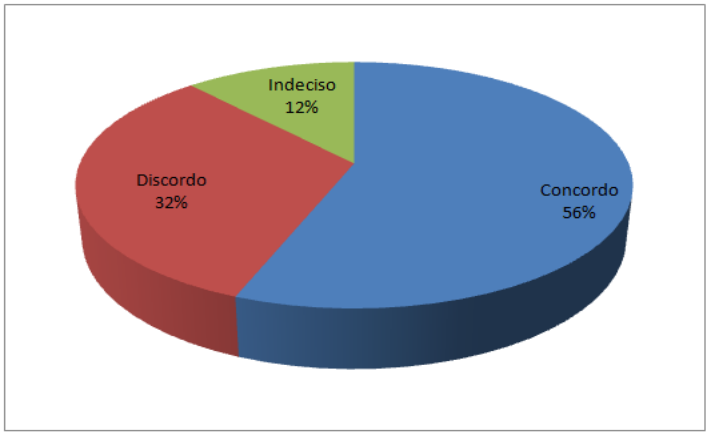

Gráfico 15. Existência de procedimentos para verificação de privilégios e bloqueios de usuários

Fonte: elaborado pelos autores

Sabendo do valor que as informações têm no mercado e do aumento da capacidade de exploração de vulnerabilidades, já era de se esperar que as empresas venham sofrendo ataques ao seu ambiente computacional. Este fato foi comprovado quando 47% das empresas afirmaram ter sofrido algum tipo de ataque aos 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% afirmam não ter sofrido ataques. Tais números são bastante semelhantes às respostas de Gabbay (2003): 45% sofreram ataques, 33% não sofreram e 21% não souberam responder.

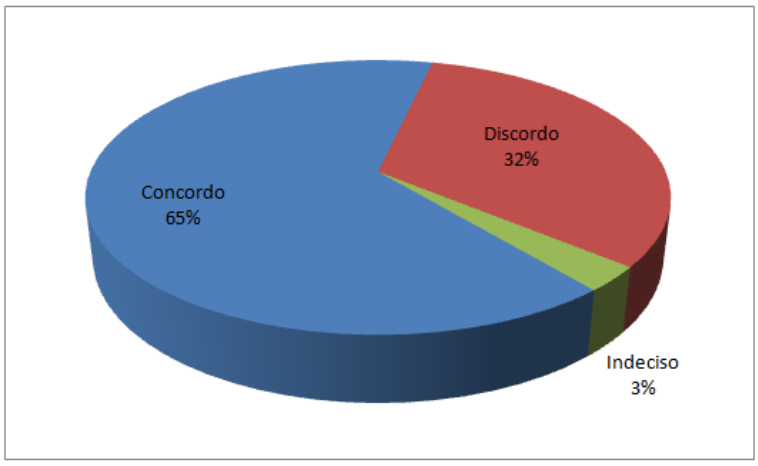

Gráfico 16. Obrigatoriedade de utilização de senhas fortes, sem repetição e com trocas periódicas

Fonte: elaborado pelos autores

Dentre as empresas que afirmaram ter sofrido algum tipo de ataque aos recursos tecnológicos ou as informações internas, 50% responderam que foi possível descobrir as vulnerabilidades exploradas, 29% não descobriram e 21% não souberam responder. Ainda abordando o mesmo grupo, 34% conseguiram descobrir a origem do ataque (Gráfico 17).

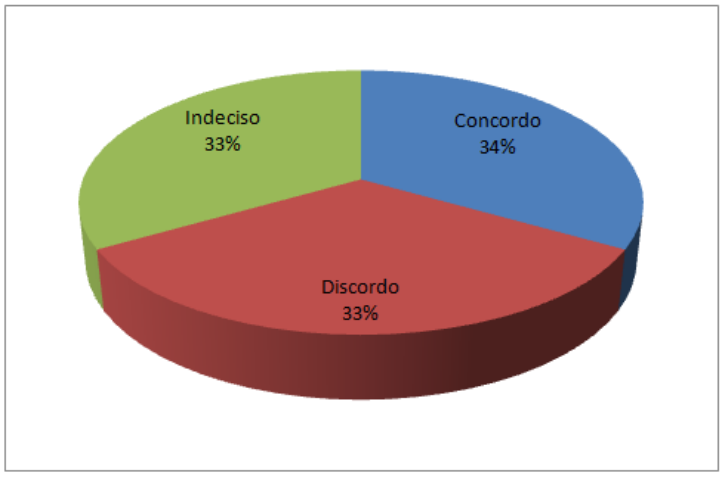

Gráfico 17. Descoberta da origem do ataque

Fonte: elaborado pelos autores

Continuando a considerar apenas as empresas que afirmaram ter sofrido algum tipo de ataque ou ficaram indecisas a esse respeito, 46% dos respondentes souberam informar as pessoas envolvidas no ataque, sendo 21% gente sem ligação direta com a empresa e 25% de *insiders* (Gráfico 18), 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 imagina (SCHNEIER, 2007). O índice maior de *insiders* também é percebido no relatório da Modulo (2006).

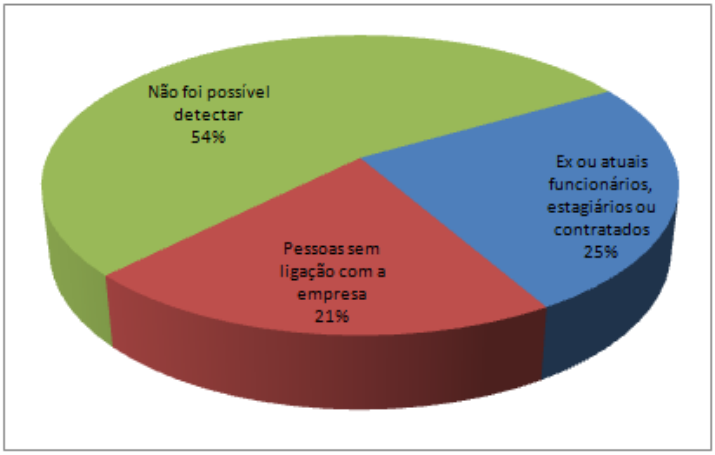

Gráfico 18. Descoberta da origem das pessoas envolvidas nos ataques

Fonte: elaborado pelos autores

Neste mesmo grupo, ao se 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, sendo exposição de informações confidenciais (67%) e perdas operacionais (58%), que tiveram maior incidência na pesquisa (Gráfico 19). Na pesquisa do Ecrime (2010), a reposta que recebeu mais indicações foi a perda operacional, seguida pelos prejuízos financeiros, danos à reputação e roubo de dados sensíveis.

Gráfico 19. Principais perdas geradas pelos ataques sofridos

Fonte: elaborado pelos autores

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 foi capaz de quantificar as perdas era bem menor (33%).

Diante deste cenário, é visível a necessidade de melhorias no ambiente até mesmo na área de tecnologia (parte da trinca essencial de TI mais fortalecida), visto que não se tem uma correta gestão dos incidentes como adverte Contos (2006), pois, mesmo tendo índices, de certa forma, bons na utilização de ferramentas (Gráfico 6), que remetem à primeira fase da gestão de incidentes (CONTOS, 2006), não se tem as demais fases bem definidas e implantadas para melhor gerência dos fatos ocorridos, como demonstram os Gráficos 17, 18 e 19.

Finalizando a pesquisa, foi possível perceber que todas as empresas têm medidas de segurança planejadas para os próximos doze meses na corporação, o que demonstra, de certa forma, consciência da situação. Entre as principais ações citadas como planejadas, percebe-se um foco mais macro para os projetos de SI corporativa, o que também foi demonstrado na pesquisa da Modulo (2006). O questionamento foi liderado por respostas como: análise de vulnerabilidades (47%), análise de risco no ambiente de TI (47%), adequação a normas, regulamentação ou legislação (41%), capacitação em SI (35%) e política de segurança da informação (32%). Tais informações são apresentadas e complementadas no Gráfico 20.

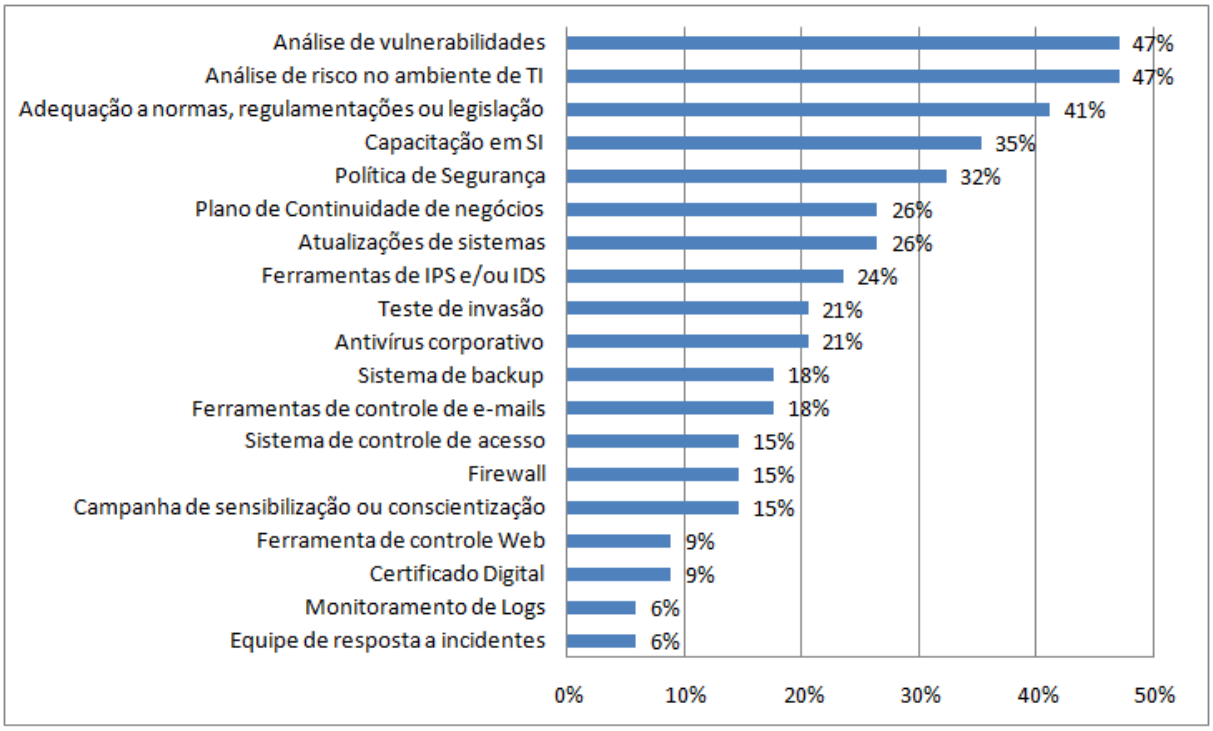

Gráfico 20. Principais medidas de segurança planejadas para os próximos 12 meses

Fonte: elaborado pelos autores

4.6 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 tomadas para que tais problemas sejam mitigados. Contudo, não são realizadas as ações e precauções necessárias, muitas vezes simples. Isto corrobora o estudo de Shay *et al*. (2010), que observa 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, já que, na maioria dos itens, não se teve assinalada a melhor alternativa, na visão da segurança da informação. Esta situação foi gerada, principalmente, no caso dos órgãos públicos, que demonstraram índices que, quando se diferenciavam dos obtidos pela iniciativa privada, eram, em sua maioria, bem inferiores, o que já havia sido identificado na pesquisa da Modulo (2006).

A pesquisa relata que 44% das empresas trata o assunto segurança da informação com a devida relevância. O tema SI vem sendo debatido de forma sistemática, embora sem que se atribua a ele a devida relevância, conforme consideram 82% das empresas. Em decorrência, não se vê sua aplicação prática, pois apenas 35% ressaltaram a existência da divulgação institucional da SI na empresa e em apenas 15% dos casos 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 verificação de privilégios e bloqueios de usuários de rede, obrigatoriedade de utilização de senhas fortes, sem repetição e com trocas periódicas, também não atingiram valores considerados satisfatórios.

Com relação aos *insiders*, percebeu-se a participação ativa de ameaças em um ambiente com características que facilitam tais fatos, visto que as empresas pesquisadas não atentam, ainda, para tal ameaça com o grau de importância que deveriam, ocorrendo falhas ou falta de procedimentos para a possível detecção dos *insiders*, desde a sua contratação. Os procedimentos, metodologias e ferramentas internas, em sua maioria, não estão seguindo as melhores práticas, nem utilizando tecnologias mais avançadas de proteção. Atividades simples de capacitação, requisitos de senhas, políticas de permissões em estações, entre outras, são ignoradas.

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 verificação dos direitos de acesso de cada pessoa ou perfil. 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 estejam todos cientes da concessão. Esses direitos devem ser retirados 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 (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. Deve-se prover de meios que incentivem as pessoas a reportar fatos que possam ser nocivos à empresa. 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 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 há 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 ressaltam 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 pode detectar possíveis *insider*s, como retratam 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 nove delas (três públicas e seis privadas). Ao ser questionado se a estratégia citada conseguiria 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 pessoas mal intencionadas. Com relação às dificuldades na implantação de um plano de segurança mais abrangente, que envolva os pontos da estratégia apresentada, os principais resultados 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% levantaram 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 terem sido incluídos em uma questão aberta e existindo a possibilidade de citar mais de um problema.

6 CONSIDERAÇÕES FINAIS

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 à área humana, como pôde 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 secundário, focado no tratamento de *malwares* e ataques externos, não se 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 a uma estratégia que contemple os processos, tecnologias e, principalmente, as pessoas em todas as suas fases, incluindo os aspectos psíquicos e sociais já abordados. Tal estratégia servirá não apenas para mitigar as ameaças internas, mas também como uma forma de prover um ambiente mais seguro, implementando a segurança de forma mais holística.

Como já abordado no trabalho, a segurança da informação ainda necessita de muitas ações e pesquisas para suprir demandas reprimidas da área, assim como para analisar novos problemas que surgem com novas ameaças e técnicas de ataque, além dos novos problemas gerados pelas próprias soluções propostas. Desta forma, acredita-se que este trabalho poderá ganhar novas contribuições e desdobramentos se estudos futuros analisarem aspectos como:

- modelos para divulgar a SI para as pessoas da corporação, mensurando o seu conhecimento;
- aprimoramento do questionário e aplicação a uma quantidade maior de empresas divididas por ramos, de forma a entender cada ambiente e prover soluções mais adequadas para cada caso;
- aplicação da teoria dos jogos para análise dos ambientes e estratégias para solucionar problemas da SI como, por exemplo, divulgação corporativa da SI, criação e aplicação da política de segurança da informação.
- Integração de pesquisas das áreas de humanas e saúde aos trabalhos de TIC de forma a se obter melhores meios para detecção e prevenção dos comportamentos dos *insiders*.

REFERÊNCIAS

ABNT. NBR ISO/IEC 17799:2001: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

ABNT. NBR ISO/IEC 27002:2005: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ALEXANDRIA, J. C. S. Gestão da segurança da informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente

de pesquisa científica. 2009. Tese - Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009.

BADDELEY, M. Herding, social influence and economic decision-making: socio-psychological and neuroscientific analyses. *Philosophical Transactions of the Royal Society. Biological Sciences*, n. 365, p. 281-290, 2010.

CASTELLS, M. *Era da informação: a sociedade em rede.* São Paulo: Paz e Terra, 2007.

CERT. Insider threat research. Pittsburgh – EUA: CERT Program, 2013. Disponível em: http://www.cert.org/insider_threat/more.html. Acesso em: 17/07/2013.

CEZAR, A.; CAVUSOGLU, H.; RAGHUNATHAN, S. Outsourcing information security: contracting issues and security implications. In: Workshop on the Economics of Information Security, 9., Cambridge - EUA. *Anais...* Harvard University, 2010.

CONTOS, B. T. *Enemy at the Water Cooler:* real-life stories of insider threats and enterprise security management countermeasures. EUA: Editora Elsevier Science, 2006.

DEL-BEN, C. M. Neurobiologia do transtorno de personalidade anti-social. *Revista de Psiquiatria Clínica*, v. 32, n. 1, p. 27-36, 2005.

ECRIME. CyberSecurity watch survey: cybercrime increasing faster than some company defenses. *CSO Magazine*, CERT Program, Deloitte, U.S. Secret Service, 2010. Disponível em: http://www.cert.org/archive/pdf/ ecrimesummary10.pdf. Acesso em: 04/07/2013.

ELLWANGER, C. Impacto da utilização de técnicas de endomarketing na efetividade das políticas de segurança da informação. 2009. Dissertação – Centro de Tecnologia, Universidade Federal de Santa Maria, Santa Maria, 2009.

FLAXMAN, E. The Cambridge spies: treason and transformed ego ideals. *The Psychoanalytic Review*, v. 97, p. 607-631, agosto, 2010.

GABBAY, M. S. 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. 2003. Dissertação – Centro de Tecnologia, Universidade Federal do Rio Grande do Norte, Natal, 2003.

GELLES, M. Exploring the mind of the spy. Texas – EUA: Texas A&M University Research Foundation. 2012. Disponível em: http://rf-web.tamu.edu/security/ security%20guide/Treason/Mind.htm. Acesso em: 07/01/2012.

GIL, A. C. *Como elaborar projetos de pesquisa*. São Paulo: Editora Atlas, 2010.

GREITZER, F. L.; MOORE, A. P.; CAPPELLI, D. M.; ANDREWS, D. H.; CARROLL, L. A.; HULL, T. D. Combating the insider cyber threat. *IEEE Security & Privacy*, v. 6, n. 1, p. 61-64, Janeiro/Fevereiro, 2008.

GUALBERTO, E. S.; SOUSA Jr, R. T.; DEUS, F. E. G.; DUQUE, C. G. InfoSecRM: uma abordagem ontológica para a gestão de riscos de segurança da informação. In: VIII Simpósio Brasileiro de Sistemas de Informação, São Paulo. *Anais...* Universidade de São Paulo: SBC, 2012.

IMPERVA. The anatomy of an insider: bad guys don't always wear black. Redwood Shores – EUA: Imperva, 2009. Disponível em: http://www.imperva.com/ docs/WP_Anatomy_of_an_Insider.pdf. Acesso em: 30/08/2013.

IMPERVA. Five signs your file data is at risk. Redwood Shores – EUA: Imperva, 2010. Disponível em: http://www.imperva.com/docs/WP_Five_Signs_Your_File_Data _is_at_Risk.pdf. Acesso em: 30/08/2013.

MACCARTHY, M. Information Security Policy in the U.S. Retail Payments Industry. In: Workshop on the Economics of Information Security, 9., Cambridge - EUA. *Anais...* Harvard University, 2010.

MARCIANO, J. L. P. Segurança da informação: uma abordagem social. 2006. Tese – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006.

MARCIANO, J. L.; MARQUES. M. L. O enfoque social da segurança da informação. *Ciência da Informação*, *Brasília*, v. 35, n. 3, p. 89-98, Dezembro, 2006.

MARCONI, M. A.; LAKATOS, E. M. *Fundamentos da metodologia científica*. São Paulo: Editora Atlas, 2010.

MÓDULO. Pesquisa nacional de segurança da informação. 10. ed. Módulo Technology for Risk Management, 2006. Disponível em: http://www.modulo.com.br/ media/10a_pesquisa_nacional.pdf. Acesso em: 21/07/2013.

MOORE, T.; CLAYTON, R.; ANDERSON, R. The economics of online crime. *Journal of Economic Perspectives*, v. 23, n. 3, p. 3-20, Summer, 2009.

MOTIEE, S.; HAWKEY, K.; BEZNOSOV, K. Do Windows users follow the principle of least privilege? Investigating user account control practices. In: Symposium on Usable Privacy and Security, 6., Redmond - EUA. *Anais...* Carnegie Mellon University,2010.

NAKAMURA, E. T.; DE GEUS, P. L. *segurança de redes em ambientes corporativos*. São Paulo: Novatec, 2007.

NOBRE, A. C. S. Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação: um estudo com gestores públicos estaduais no Brasil. 2009. Dissertação – Departamento de Ciências Administrativas, Universidade Federal do Rio Grande do Norte, Natal, 2009.

RAMOS, I. Q. Contribuição da Ciência da Informação para criação de um plano de segurança da informação. 2007. Dissertação – Centro de Ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas, 2007.

RAYWOOD, D. Number of employees who would steal data increase significantly. *SC Magazine UK*, 2010. Disponível em: http://www.scmagazineuk.com/number-of-employees-who-would-steal-data-increases-significantly/article/191472/. Acesso em: 24/07/2013.

RIGON, E. A.; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 1, artigo 3, jan-mai, 2013.

ROHR, A. Funcionário do Bank of America instala vírus em caixas eletrônicos. *Linha Defensiva*, 2010. Disponível em: http://www.linhadefensiva.org/2010/04/funcionario-do-bank-of-america-instala-virus-em-caixas-eletronicos/>. Acesso em: 20/07/2013.

SCHNEIER, B. BT Counterpane's founder and chief technology officer talks to SA Mathieson at Infosecurity Europe. *InfoSecurity Magazine*. 2007. Disponível em: http://www.schneier.com/news-040.html. Acesso em: 22/07/2013.

SCHNEIER, B. The psychology of security. 2008. Disponível em: http://www.schneier.com/essay-155.html. Acesso em: 22/07/2013.

SERAFIM, A. P. Investigação psicológica da personalidade na conduta criminosa. In: RIGONATTI, S. P.; SERAFIM, A. P.; BARROS, E. L. (Org.). *Temas em Psiquiatria Forense e Psicologia Jurídica*. São Paulo: Editora Vetor, 2003.

SHAY, R.; KOMANDURI, S.; KELLEY, G. K.; LEON, P. G.; MAZUREK, M. L.; BAUER, L.; CHRISTIN, N.; CRANOR, L. F. Encountering stronger password requirements: user attitudes and behaviors. In: Symposium on Usable Privacy and Security, 6., Redmond - EUA. *Anais...* Carnegie Mellon University, 2010.

SHIELS, M. BBC News. Malicious insider attacks to rise. BBC News UK, 2009. Disponível em: http://news.bbc.co.uk/2/hi/technology/7875904.stm. Acesso em: 03/08/2013.

STAFF, SC. Recession could cause employees to steal data to help themselves or others. *SC Magazine UK*, 2009. Disponível em: http://www.scmagazineuk.com/ recession-could-cause-employees-to-steal-data-to-help-themselves-or-others/article/158300/. Acesso em: 27/07/2013.

SULLIVAN, R. J. The changing nature of U.S. card payment fraud: issues for industry and public policy. In: Workshop on the Economics of Information Security, 9., Cambridge - EUA. *Anais...* Harvard University, 2010.