VIII ENANCIB – Encontro Nacional de Pesquisa em Ciência da Informação
28 a 31 de outubro de 2007 • Salvador • Bahia • Brasil

GT 4 – Gestão da Informação e do Conhecimento nas Organizações
Pôster

PERCEPÇÕES DE SEGURANÇA E AMEAÇAS EM AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO

PERCEPTION OF SECURITY AND THREATS IN ENVINROMENT OF INFORMATION TECHNOLOGY

Miguel Maurício Isoni (CCSA/UFPB, miguelisoni@uol.com.br)
Silvana Aparecida Borsetti Gregório Vidotti (PPGCI/UNESP, vidotti@marilia.unesp.br)

Resumo: Invadir privacidades e prejudicar o fluxo das informações são anomalias corriqueiras em ambientes de tecnologia da informação. As violações tornaram-se sofisticadas e inteligentes apontando para uma escalada de perdas financeiras diretas causadas por delitos diversos. Com objetivo de mapear as percepções quanto à origem dos ataques, descontinuidades dos processos e interrupção do fluxo das informações, uma pesquisa de caráter quantitativo foi realizada, que resultou neste presente artigo, tendo como público-alvo participantes de um evento em segurança da informação.
Palavras-chave: Segurança da informação. Ameaças. Origem dos ataques. Códigos maliciosos. Interrupção do fluxo das informações.

Abstract: *Invading privacy and harming the flow of information are current anomalies in environment of information technology. The violations had become sophisticated and intelligent pointing to an escalation of direct financial losses caused by several crimes. With the objective of mapping the perceptions concerning the origin of the attacks, process discontinuities and interruption of the flow of information, a research of quantitative character was realized, which resulted in this present article, having as a public target participants in an event of information security.*
Keywords: *Information security. Threat. Origin of the attack. Malware. Interruption of the flow of information.*

1 Escopo e objetivo da pesquisa

Segurança, em geral, pode ser alcançada através da prevenção, preensão, inibição, desvio, bem como, detecção de ataques e contramedidas de proteção e eliminação de intrusão. E a detecção da invasão é baseada nas crenças de que o comportamento de um intruso será noticiavelmente diferente do de um usuário legítimo e de que muitas ações não-autorizadas são detectáveis (MUKHERJEE et al., 1994).

A fim de conhecer as percepções de gerentes, administradores, especialistas e estudiosos de sistemas e redes computacionais, relacionadas as falhas ocasionadas por ações maliciosas, foi conduzida uma pesquisa quantitativa, validada por análises de variâncias e mapas de perceptivos, com a interpretação dos resultados, que resultou no presente artigo.

Tratando da concordância ou discordância de questões que caracterizam a origem dos ataques e as ameaças que ocasionam a interrupção do fluxo de informação, este trabalho de pesquisa é também parte integrante de um projeto de estudos e investigações em Ciência da Informação.

2 Metodologia da pesquisa

A pesquisa foi construída a partir de dados primários coletados junto aos participantes do 8º. Simpósio de Segurança em Informática – SSI-2006, realizado em São José dos Campos, São Paulo, no período de 8 a 10 de novembro de 2006, no Instituto Tecnológico da Aeronáutica – ITA. Metodologicamente, ficou determinado que a pesquisa tivesse também caráter exploratório com questões conclusivas descritivas.

Com autorização da coordenação geral do SSI-2006, os questionários foram distribuídos aos participantes juntamente com a pasta do simpósio. Alguns questionários respondidos foram entregues na secretaria do evento, conforme instrução contida no instrumento e, outra significativa parte dos questionários foi obtido e recolhidos através de abordagem pessoal durante as palestras, mini-cursos e intervalos da programação.

O instrumento da pesquisa ficou dividido em duas partes. A primeira parte consta de uma breve explicação da finalidade do questionário seguida de alguns dados sobre a caracterização dos sujeitos, com intuito de estratificar a amostra e escalonar as percepções do público-alvo.

Na segunda parte do instrumento ficaram as questões estruturadas por uma escala de intervalo, com valores de 1 a 10. Os respondentes, dessa forma, atribuíram um grau de concordância, em relação às afirmativas propostas, em cada uma das questões. A cada célula de resposta foi atribuído um número que refletia a direção da atitude do respondente em relação a cada afirmação, permitindo assim classificar as percepções de concordância em três níveis: baixa – intervalo de 0 a 4; média – intervalo de 5 a 7; e alta – intervalo de 8 a 10. Esses degraus de concordância permitiram um cruzamento estatístico e a construção dos mapas perceptuais para cada questão da pesquisa.

A amostra foi formada por 177 respondentes com as características e estratificações apresentadas nas Tabelas 1 e 2. Os dados tabulados foram organizados em uma planilha e convertidos para um sistema estatístico, que permitiu a realização da aplicação de técnicas para a análise e validação dos dados.

A estratificação dos respondentes, descritas na Tabela 1, obedeceu ao critério do cargo que o mesmo ocupa, descritos pelo nome (grifado) de maior importância e que representa o perfil que mais se aproxima de suas responsabilidades, distribuídos como: executivo, gerente, ou

tomador de decisões; programador, técnico ou analista; pesquisador, professor ou estudante de pós-graduação; e por último, aluno de graduação ou graduado. Os respondentes foram instruídos a escolher, dentre as opções de cargos, aquele que mais lhe absorve tempo, atenção e envolvimento, pois alguns acumulam mais de uma atividade funcional.

TABELA 1
Distribuição do cargo dos respondentes.

Cargo	n	%
Executivo	35	19,8
Programador	95	53,7
Pesquisador	28	15,8
Aluno	19	10,7
TOTAL	177	100,0

Fonte: Dados da pesquisa

De acordo com a Tabela 1, os respondentes de maior freqüência foram os programadores que participaram da pesquisa com 53,7% das respostas. Em segundo lugar ficaram os executivos, correspondendo a 19,8%. É importante destacar que a soma da participação dos programadores e executivos representa mais de 70% da amostra. São os programadores/analistas os responsáveis pela administração dos sistemas e das tecnologias – sendo assim, os que mais enfrentam as questões de segurança. E, são os executivos de TI que têm na segurança uma de suas maiores preocupações.

A distribuição das questões foi dividida em duas seções, conforme Tabela 2. A primeira seção para apurar a percepção sobre ataques, erros, falhas, fraudes e roubos; e, a segunda, sobre a percepção de segurança do fluxo de informação entre a fonte e o destino.

TABELA 2
Distribuições das questões

Os ataques, erros, falhas, fraudes e roubos são provenientes com maior intensidade:	
Q1	de pessoal interno (dentro da organização).
Q2	de pessoal externo (fora da organização).
Na segurança do fluxo de informação entre a fonte e o destino existem várias ameaças e ataques. Em sua opinião o que mais ocorre:	
Q3	interrupção do fluxo por ataque a disponibilidade da informação
Q4	interceptação da informação através de ataque a confidencialidade
Q5	por modificação de conteúdo pelo ataque a integridade dos dados
Q6	por fraude ou violação através de ataque a autenticidade da informação
Q7	por intrusão (worms, phishing etc) através do uso de códigos maliciosos
Q8	por interrupção de serviço através de ataques por DoS (Denial of Service)

Fonte: Dados da pesquisa

Entre as oito variáveis analisadas, apenas Q_4 - interceptação da informação através de ataque à confidencialidade - não apresentou variabilidade significativa por cargo (Valor-P < 0,05). Sendo assim, a análise de variância e de correspondência para Q_4 foi abandonada. Nas

demais variáveis, Q_3, Q_5, Q_6, Q_7 e Q_8 ficaram validadas e evidenciadas, de forma estatística, com uma significativa variação de concordância das respostas por cargo.

3 Validação das respostas

De posse da estratificação da amostra, procedeu-se à validação das respostas distribuídas por cargo e grau de concordância baixa, média e alta. Esclareça-se que a proveniência dos ataques, a segurança do fluxo de informação e as percepções de possíveis atuações pró-ativas, durante e depois dos ataques perpetrados, compõem o foco dos resultados esperados.

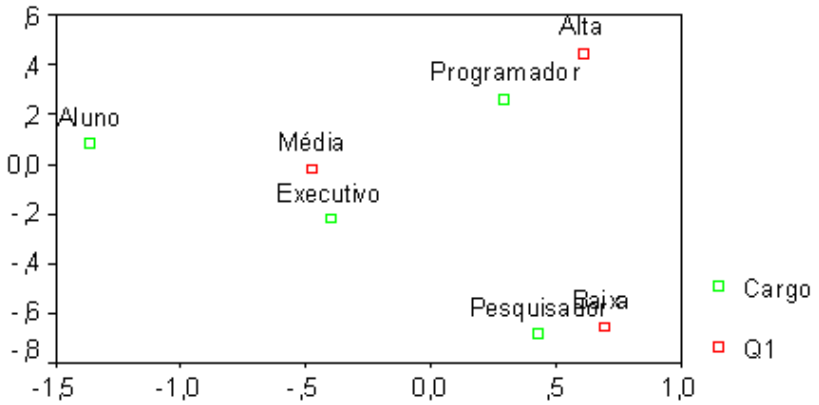
A cada célula de resposta foi atribuído um número que reflete a direção da atitude do respondente em relação a cada afirmação, permitindo assim classificar as percepções em três níveis, quais sejam: "Baixa" – intervalo de 0 a 4; "Média" – intervalo de 5 a 7; e "Alta" – intervalo de 8 a 10. Esses graus de concordância ("Baixa", "Média" ou "Alta"), permitiu um cruzamento estatístico e a construção dos mapas perceptuais mostrados a seguir.

3.1 A percepção da origem dos ataques

As análises de correspondências para Q_1 e Q_2, apresentadas pelas figuras 1 e 2, respectivamente, provêm um mapa visual que realça a comparação dos atributos "baixa", "média" e "alta" em um espaço perceptual, avaliando o grau de concordância por cargo.

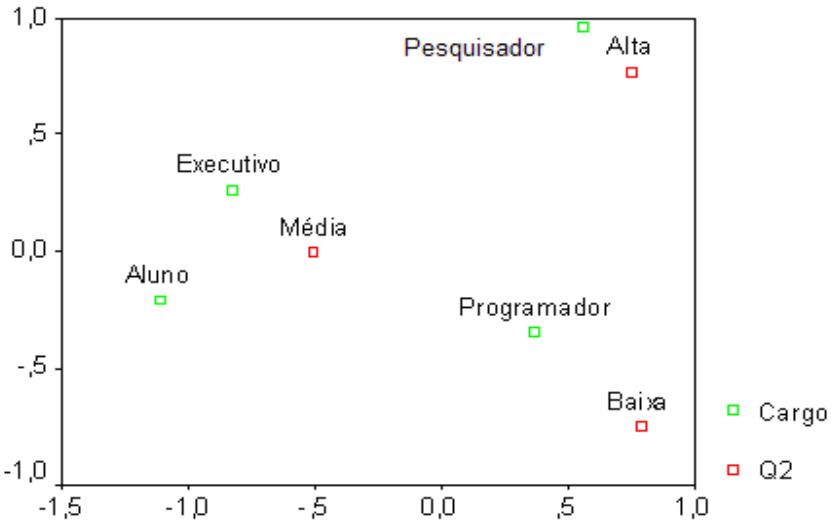
Observa-se na Figura 1 a proximidade do programador com o grau de concordância "alta" e a proximidade do pesquisador com o grau de concordância "baixa". Isto quer dizer que, quando se questiona a origem dos ataques, os programadores concordam fortemente que os ataques são provenientes de fora da organização. Por outro lado, os pesquisadores concordam fracamente com esta afirmativa.

FIGURA 1
Análise de Correspondência para a Q_1 e cargo



Já Figura 2 as conclusões ficam invertidas, pois os pesquisadores concordam fortemente que os ataques são provenientes de fora das organizações, enquanto os programadores concordam fracamente com esta afirmativa. Para os pesquisadores as vulnerabilidades ocorrem de fora para dentro em decorrência do volume significativo de acessos e trocas de informações existentes na Internet.

FIGURA 2
Análise de Correspondência para a Q_2 e cargo.



3.2 Percebendo as ameaças que afetam o fluxo das informações

As ameaças que comprometem o fluxo de informação e corrompem o processamento precisam ser identificadas. Essas ameaças ocorrem pela execução de código malicioso e pela divulgação não autorizada de informações confidenciais. A Tabela 3 apresenta a distribuição percentual para grau de concordância "Alto", a fim de posicionar um escore entre as ameaças relacionadas as interrupções do fluxo das informações.

TABELA 3
Percentual de concordância "alto" para as afirmativas Q_3 a Q_8.

Afirmativa	n	%
Q_3	35	19,8
Q_4	35	19,8
Q_5	24	13,6
Q_6	42	23,7
Q_7	127	71,8
Q_8	91	51,4

Fonte: Dados da pesquisa

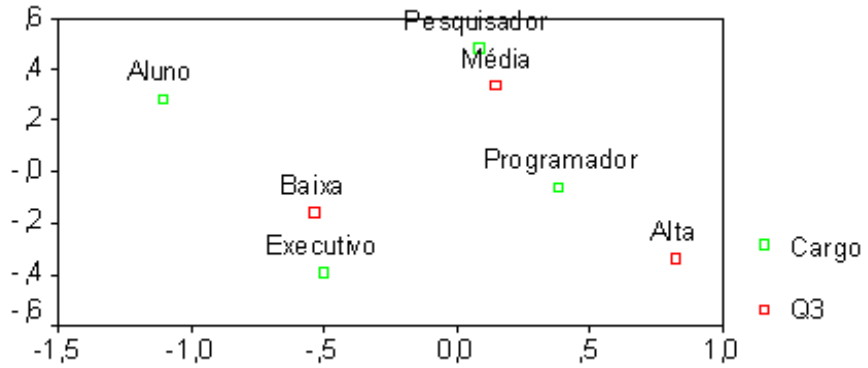
Observa-se na Tabela 3 que a afirmativa Q_7 (71,8%) possui o maior percentual de concordância alta entre todos os respondentes, ou seja, eles percebem mais fortemente que os ataques são provenientes por intrusão através do uso de códigos maliciosos. A afirmativa Q_8 (51,4%), que se refere a interrupção do fluxo das informações originado pelo ataque de "negação de serviços" (DoS), aparece em segundo lugar na percepção dos respondentes. *Denial of Service*[i] (DoS) – negação de serviços, são tentativas de impedir usuários legítimos de utilizarem um determinado recurso, por exemplo, com interrupção de serviços da Internet, por uma inundação de tráfego falso que entope a rede do provedor

Com diferenças de estratégia de ataque, evidencia-se que as questões de Q_3 a Q_8, que se propõem exploratórias, obedecem a uma mesma indagação sobre a quebra do fluxo das informações.

3.3 Ataques à disponibilidade, à integridade e à autenticidade das informações

A fim de realizar uma avaliação comparativa do grau de concordância por cargo na percepção dos respondentes, as Análises de Correspondências – os mapas perceptivos, para as questões Q_3, Q_5 e Q_6, estão sucessivamente apresentados pelas figuras 3, 4, 5, para as altas, médias e baixas concordâncias.

FIGURA 3
Análise de correspondência para a variável Q_3 e cargo.



A visualização dos mapas, representados pelas figuras 3, 4 e 5, não deixa dúvida sobre a percepção que cada grupo de respondente teve em relação aos parâmetros de concordância para as variáveis Q_3, Q_5 e Q_6. Veja, por exemplo, o posicionamento dos pesquisadores em função das variáveis Q_3 e Q_5 – ficando bem próximos à concordância média, ou a dos executivos que percebem em Q_6 uma concordância alta.

FIGURA 4
Análise de correspondência para a variável Q_5 e cargo.

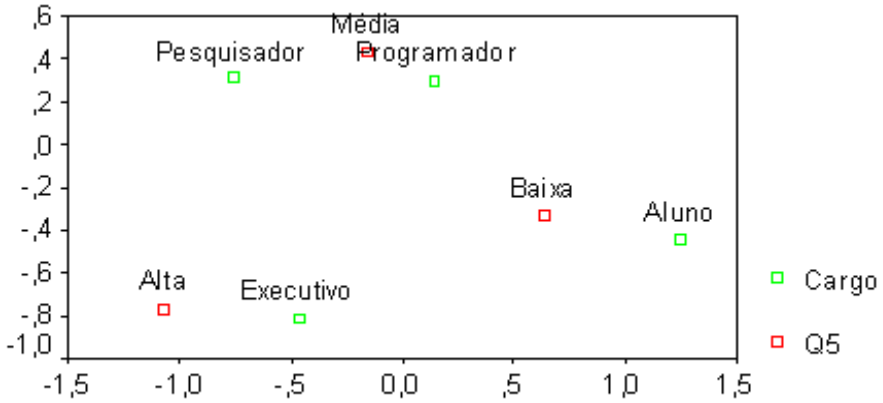
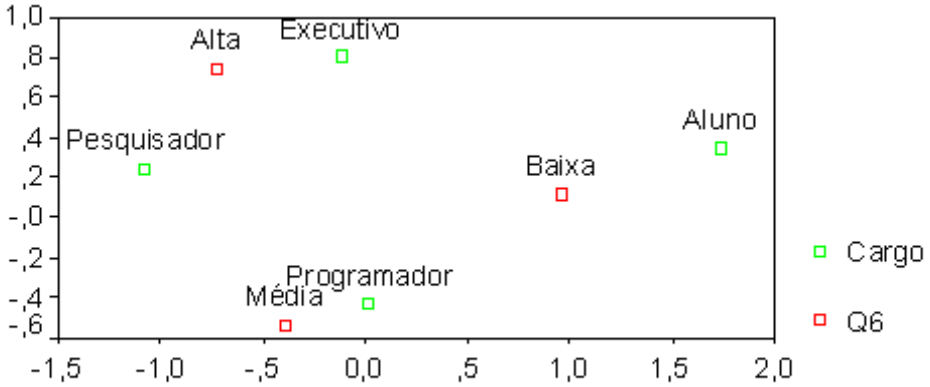


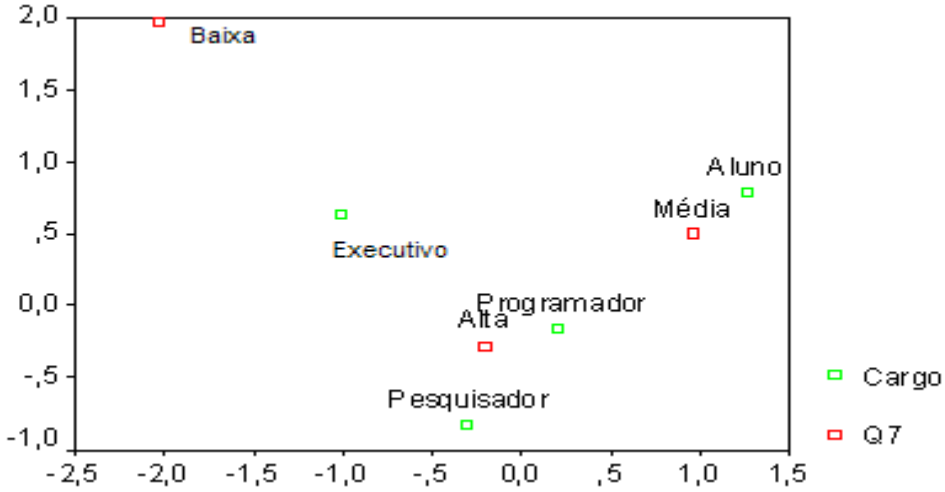
FIGURA 5
Análise de correspondência para a variável Q_6 e cargo.



3.4 Ataques provenientes de códigos maliciosos ou negação de serviços

A Figura 6 apresenta a análise de correspondência para a variável Q_7, e nela podemos visualizar primeiro, que a concordância baixa é desprezível na percepção do conjunto de todos os respondentes; e, segundo, que executivos, programadores e pesquisadores estão próximos e ligados fortemente pela concordância alta de que este tipo de ataque é o que mais ocorre nos ambientes de TI; e, finalmente, de que a falta de prática e conhecimento dos respondestes alunos os caracteriza como inexperientes na percepção dessa variável de ameaça.

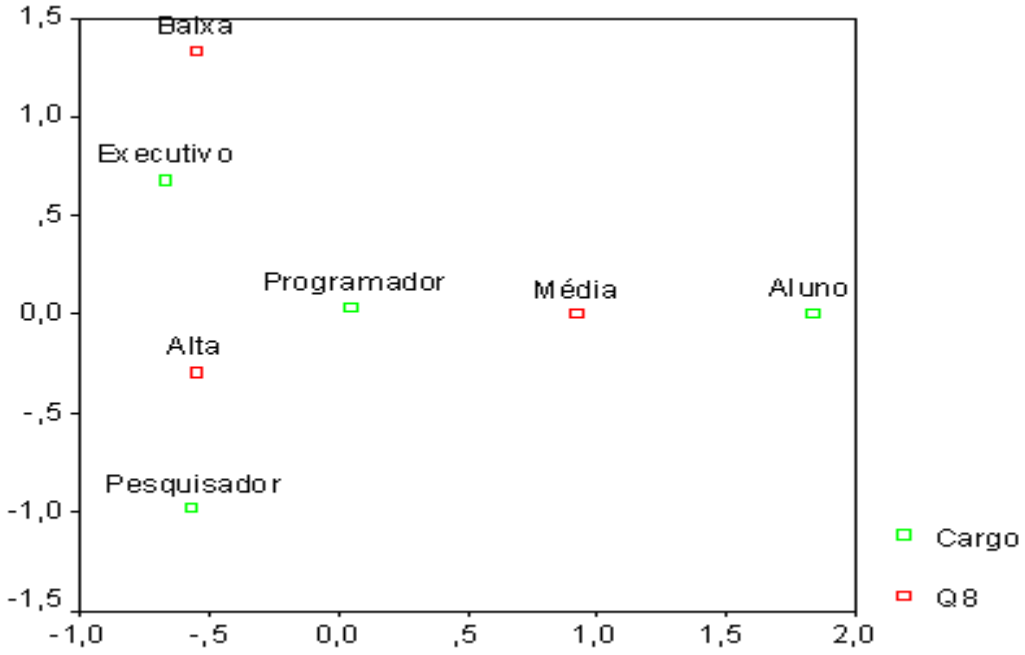
FIGURA 6
Análise de correspondência para a variável Q_7 e cargo.



De acordo com a Figura 7, que apresenta a análise de correspondência para a variável Q_8, pode-se considerar um agrupamento (*cluster*) dos cargos Executivo (60%), Pesquisador (82,1%) e Programador (49,5) em torno do nível de alta concordância.

FIGURA 7

Análise de correspondência para a variável Q_8 e cargo.



4. Interpretação dos Resultados

"*Onde estão ou podem estar as ameaças?*" - indaga Leonardo Scudere (2007, p.45) - que conclui que estariam no público interno da rede corporativa. Este público é chamado por ele de usuários confiáveis, com os quais estão a fonte de quase todos os ataques, ou seja, "*as ameaças podem partir de qualquer um dos componentes dessa cadeia segmentada e dinâmica que compõem a empresa estendida e que podem comprometer todo valor e credibilidade de um negócio*" (SCUDERE, 2007, p.46). Scudere (2007, p.44) considera a "*empresa estendida*" como toda a cadeia de valor que interage através de um ambiente tecnológico, abrigando não só o negócio principal, como também clientes, fornecedores, parceiros, sub-contratados e terceiros em geral.

Cansian (2001, p.144) analisa o perfil do atacante por dois padrões: "*aqueles provenientes do meio interno, oriundos da própria organização, empresa ou instituição, e os atacantes externos, normalmente provenientes da Internet*". O autor afirma ainda que o atacante interno é dotado de um comportamento mais complexo, "*demonstrando na maioria das vezes a mesma motivação dos crimes regulares, ou seja*: *cobiça, obtenção ilegal de dinheiro, lucro, riqueza, ou até mesmo ligados a revanches pessoais ou vingança*" (CASIAN, 2001, p.145).

Pesquisa conduzida pela *Computer Security Institute* – CSI – com auspício do *Federal Bureau of Investigation's* (FBI) - *Computer Intrusion Squad* (GORDON et al, 2005), com o intuito de levantar dados e características dos crimes cibernéticos, mostrou que a maioria dos ataques que envolvem perdas financeiras ocorre ou contam com a cooperação de alguém de dentro das próprias organizações atacadas.

Analisando a pesquisa aplicada aqui relatada, pode-se inferir as variáveis Q_1 e Q_2, que tratam da origem dos ataques, que os pesquisadores possuem uma visão externa da organização e sabem que a engenharia social, a criatividade e sofisticação das ameaças provêm do

comportamento criminoso típico em nossa sociedade. Para eles a origem dos ataques vem do meio externo, onde seus principais esforços de estudos e pesquisas se concentram. Na opinião dos pesquisadores, está principalmente no fluxo da rede uma das perspectivas de soluções para minimizar os constantes ataques de códigos maliciosos.

Diferentemente, os respondentes programadores percebem que as ameaças surgem de dentro das organizações, pois além de ter uma visão cotidiana da administração dos recursos de TI, as suas maiores preocupações estão no lado interno, pois, para eles, é nesse ambiente que se encontram as muitas fragilidades que podem ser exploradas para consecução de um ataque bem sucedido. Os programadores têm uma visão das defesas bem postadas contra ataques externos, dispondo de filtros (*firewalls*[ii]) e *softwares* de detecção de intrusão (*Intrusion Detection Systems – IDS*[iii]), recursos capazes de controlar e até mesmo impedir boa parte das ameaças provenientes de fora de sua base tecnológica.

Os executivos, de outra forma, se posicionam em um meio termo, isto é, com uma percepção comedida. Eles tomam uma posição de equilíbrio em relação às variáveis Q_1 e Q_2, o que significa que ambos os cenários (ataques internos ou externos) merecem sua atenção. Já os alunos se encontram deslocados dos graus de concordância, pela sua inexperiência perceptiva da questão.

Através da distribuição do grau de concordância para as varáveis Q_3 e Q_5, pode-se observar que quase todos os respondentes se mantiveram posicionados na concordância mediana. O que significa, na percepção dos respondentes, que essas ameaças existem, mas não são as que mais provocam a interrupção do fluxo das informações. Podemos até enfatizar que se ocorrer a interrupção por um desses dois motivos (Q_3 - interrupção do fluxo por ataque à disponibilidade da informação; Q_5 - por modificação de conteúdo pelo ataque à integridade dos dados), prontamente haverá a recuperação do fluxo das informações, pois disponibilidade e confidencialidade são um dos aspectos básicos da segurança e estão relacionadas com a proteção sobre informações que possuem valor.

A integridade das informações é um aspecto que garante que os dados mantenham todas as características originais. Dessa forma, do ponto de vista estatístico, o grau de concordância para Q_6 – de que o fluxo da informação pode ser interrompido por fraude ou violação através de ataque à autenticidade da informação - possui um diferencial significativo por cargo. Pode-se observar então, que executivos e pesquisadores são os que mais fortemente concordam com essa afirmativa. Na opinião de ambos, as intrusões acontecem por quebra de segurança, principalmente através da obtenção de senhas de acesso aos sistemas.

Podemos também afirmar, para as variáveis Q_3, Q_5 e Q_6, que quando se trata de aplicações criticas, as interrupções precisam ocorrer por um espaço de tempo mínimo possível e tolerável. E a recuperação do fluxo das informações poderá ocorrer pelo procedimento de *back-ups* - cópia de arquivos, ou através de política de espelhamento de *hardware* - utilizando algoritmo do tipo RAID (*Redundant Array of Independent Disks*), ou por sistemas tolerantes a falhas.

As ameaças e ataques à segurança do fluxo de informação, entre a fonte e o destino, são mais reconhecidas pelos respondentes quando se trata de intrusão através do uso de códigos maliciosos – variável Q_7, observando forte consenso entre pesquisadores, executivos e programadores. Por tanto, ataque com programas destrutivos ou maliciosos poderão abalar a reputação conquistada, minando a confiabilidade, a confidencialidade e a disponibilidade das informações, sistemas e processos.

Os ataques podem ser classificados pelo nível de automação, pela vulnerabilidade explorada, pela dinâmica e pelo impacto causado. Observando a variável Q_8 - ataques por negação de serviço - a maior concordância para este tipo de ação ocorre para pesquisadores e

executivos. Segundo a vulnerabilidade explorada, existem dois tipos de ataques de negação de serviços: os ataques aos protocolos e os ataques de força-bruta – que significa, por exemplo, a possibilidade de decodificar dados criptografados, do tipo senha, por tentativa e erro, ou seja: através de um esforço exaustivo em vez de estratégias intelectuais.

5 Considerações Finais

Pereira (2005, p.67) descreve que é "*fundamental conhecer as vulnerabilidades e fraquezas*", sejam internas ou externas ao ambiente da segurança da informação digital. Como também, acrescenta o autor, é fundamental, para mitigar os ataques e ameaças: [...] "*conhecer as possíveis conseqüências e as melhores ferramentas e práticas a adoptar para reduzir ou pelo menos prevenir e, caso se concretize ter um plano de contingência que permita uma rápida actuação e minimize as suas conseqüências*" (PEREIRA, 2005, p.68).

Vem crescendo a ocorrência daquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos fluxos das informações e a integridade dos dados.

Algumas vezes, anomalias e descontinuidades no fluxo das informações são provenientes das falhas, causadas por problemas de especificação, implementação e operação, como também por causa de defeitos, imperfeições e fadiga dos componentes, além de distúrbios externos como radiação, interferência eletromagnética e variações ambientais.

Deve ser considerado, entretanto, que um sistema tolerante a falhas deve ser também seguro a intrusões e ações maliciosas. Contudo, qualquer que seja a falha, o desafio será sempre o de prover a informação certa, para a entidade certa, no tempo certo e de maneira segura com confiabilidade e tolerância a falha a fim de minimizar impactos na interação e no fluxo das informações.

Falhas nas disponibilidades das informações não podem ser toleradas, pois as conseqüências podem ser catastróficas para a imagem e reputação institucional. Sendo assim, para que se consiga uma total confiabilidade das informações não deveria ocorrer interrupção no fluxo do serviço e nem perda de dados, o que tornaria os sistemas totalmente confiáveis e disponíveis. Mas no mundo real, confiabilidade e disponibilidade absolutas estão muito longe de serem alcançadas (WEBER, 2003).

Incrementar estratégias de promoção da segurança e redução de riscos, a fim de controlar e combater os ataques e ameaças é uma tarefa multidisciplinar envolvendo várias áreas, mas principalmente a Ciência da Informação e a Ciência da Computação. Na Ciência da Informação, além das questões de disponibilidade (como?), acesso (quem?) e recuperação da informação (o quê?), temos a ética dos usos e as garantias de privacidade, inviolabilidade e transparência na manipulação dos dados pessoais. Na Ciência da Computação, a segurança é questão intrínseca aos processos e seu ciclo de vida, desde sua especificação, desenvolvimento, implementação e manutenção até as estratégias de captura dos dados, dos códigos de tratamento e de processamento, como também as políticas de acessos restritos ou irrestritos e os planos de contingência.

REFERÊNCIAS

CANSIAN, Adriano M. **Conceitos para perícia forense computacional**. Anais VI Escola Regional de Informática da SBC, Instituto de Ciências Matemáticas e Computação de São Carlos, USP (ICMC/USP), São Carlos, SP,. p.141-156, 2001.

IDG NOW. **Há 20 anos, surgia primeiro vírus de computador.** Seção: Segurança, vírus. 20 jan 2006. Disponível em: <http://idgnow.uol.com.br/seguranca/2006/01/20/idgnoticia.2006-02-06.6845533550/IDGNoticia_view>. Acesso em: set 2006.

IMPACTA TECNOLOGIA. **Pesquisa sobre mercado corporativo de TI no Brasil**. IPM - Impacta Pesquisa Periódica de Mercado, São Paulo, maio 2005. Disponível em: <http://www.impacta.com.br/ipm/pdfs/20050531_iccorp_reembolso_analise1.pdf>. Acesso em: set 2006.

GORDON, Lawrence A. et al. **CSI/FBI - Computer crime and security survey.** Computer Security Institute Publications, Tenth Annual, 2005. Disponível em: <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf>. Acesso em: out 2006.

LUCCA, Elcio A. de. **A luta contra a fraude na Internet.** Guia Serasa de orientação ao cidadão – saiba como reduzir os riscos de vírus, hackers e outras ameaças, e ter mais segurança na Internet, 2006. Disponível em: <http://www.serasa.com.br/guiainternet/apresentacao.htm>. Acesso em: set 2006.

MUKHERJEE, Biswanath; HEBERLEIN, L. Todd; LEVITT, Karl N. **Network Intrusion Detection**. IEEE Network, v. 8, n. 3, p. 26-41, 1994.

NASCIMENTO, J. Agnaldo. **Curso de SPSS**. Programa de Pós Graduação em Administração da UFPB. JP. 2003. 45 f. Notas de aula.

PEREIRA, Pedro J. Fernandes. **Segurança da Informação Digital**. Cadernos de Biblioteconomia Arquivística e Documentação – Cad. BAD, nº 1, Lisboa, 2005, p.66-80.

SCUDERE, Leonardo. **Risco digital – como a tecnologia pode agregar valor aos negócios, criar novas oportunidades e reduzir as fraudes**. Elsevier, Rio de Janeiro, 2007.

WEBER, T. S. **Tolerância a falhas: conceitos e exemplos**. Intech Brasil, São Paulo, v. 52, p. 32-42, 2003.

[i] *Denial of Service* (DoS) – negação de serviços, são tentativas de impedir usuários legítimos de utilizarem um determinado recurso, com interrupção de serviços da Internet ou por uma inundação de tráfego falso.
[ii] *Firewall* tem por função regular o tráfego de rede e impedir a transmissão de dados nocivos ou não-autorizados de uma rede a outra.
[iii] Os *Intrusion Detection Systems* detectam violações de segurança e respondem enviando notificações de alertas..