Internet e segurança da informação: evidências de firmas e domicílios brasileiros*

Samuel César da Cruz Júnior**
Igor Siqueira Cortez***

1 INTRODUÇÃO

O economista Fritz Machlupnos (1962) denominou, ainda no século passado, a sociedade atual como a sociedade do conhecimento ou da informação, e, de fato, ele tinha toda a razão. Hoje, a informação é arma estratégica e o ativo mais valioso para qualquer organização ou indivíduo.

A sociedade da informação destaca-se pela rápida massificação das tecnologias de informação e comunicação (TIC), fomentando a convergência tecnológica, o acesso contínuo à internet e às redes sociais. Com isso, verifica-se interatividade constante entre indivíduos e dispositivos, resultando na interconexão e interdependência de sistemas.

Contudo, a explosão de produção, armazenamento e transferência de dados entre diferentes dispositivos e entre diversas redes resulta, ao mesmo tempo, em um aumento significativo das ameaças e vulnerabilidades da segurança cibernética. Se, por um lado, o aumento da tecnologia significa melhora nos sistemas, por outro, resulta em aumento de pontos de fragilidade. Redes colaborativas têm ganhado força como fonte de disseminação de ferramentas de invasão, conhecimentos necessários e troca de experiências, reduzindo cada vez mais o nível de experiência técnica necessária para se operacionalizarem ciberataques. A cada ataque bem-sucedido, os mecanismos e ferramentas são divulgados pela rede, tornando o ambiente cibernético ainda mais tenso.

Esse aumento descontrolado de atores no espaço cibernético (vale lembrar que vai além das fronteiras do Estado) tornou-se um ambiente ideal para a proliferação de *crackers*, *hackers* mal-intencionados e criminosos virtuais. Muitas vezes, os mecanismos de proteção não conseguem evoluir na mesma medida que as ferramentas de ataque.

Visto que o ciberespaço é um ambiente de disputas, é prudente dedicar especial atenção aos mecanismos de segurança da informação,[1] bem como ao comportamento dos usuários de rede. Estes mecanismos buscam garantir os requisitos mínimos para a proteção e preservação dessa grande quantidade de informação armazenada e compartilhada.

Um ciberespaço seguro favorece o desenvolvimento de mecanismos importantes para a economia do país, como o comércio eletrônico (*e-commerce*), que consegue conectar redes de clientes e fornecedores, mesmo que isolados geograficamente ou quando situados em lugares distantes. Além disso, contribui para reduzir a sobrecarga de produtos e serviços oferecidos por sistemas bancários, governamentais, entre outros.

Ameaças virtuais podem resultar em consequências reais de grande impacto se não forem tratadas adequadamente. A primeira medida para conseguir proteção contra uma ameaça cibernética é ter consciência de que ela existe e ser capaz de identificá-la quando de sua ocorrência. Um usuário que não consegue, antes de tudo, identificar um *spam*, um *phishing*, uma tentativa de intrusão ou *DoS*, certamente, está bem mais suscetível a cair nestas armadilhas e sofrer as consequências.

---

* A elaboração deste artigo só foi possível devido à cooperação entre o Ipea e o Comitê Gestor de Internet (CGI).

** Técnico de Planejamento e Pesquisa da Diretoria de Estudos e Políticas Setoriais, de Inovação, Regulação e Infraestrutura (Diset) do Ipea.

*** Pesquisador do Programa de Pesquisa para o Desenvolvimento Nacional (PNPD) no Ipea.

1. Em termos técnicos, a segurança da informação (SI) pode ser definida como a preservação da confidencialidade, integridade e disponibilidade da informação (ver ABNT NBR ISO/IEC 27001).

A decisão de investir em segurança da informação é tão importante quanto saber o quanto e como investir. Na sociedade da informação, assim como na real, todos compartilham o mesmo espaço virtual, mas o Estado é o principal ator responsável por garantir seu ordenamento, sua regulamentação, e também a segurança dos usuários.

Este texto propõe-se a analisar o comportamento dos internautas e empresas brasileiras acerca de algumas características fundamentais para uma navegação segura: experiência, preferências de navegação e mecanismos de defesa de rede. Este estudo foi realizado com base nos dados fornecidos pelo Comitê Gestor de Internet (CGI) do Centro de Estudos em Tecnologia de Informação e Comunicação (CETIC).

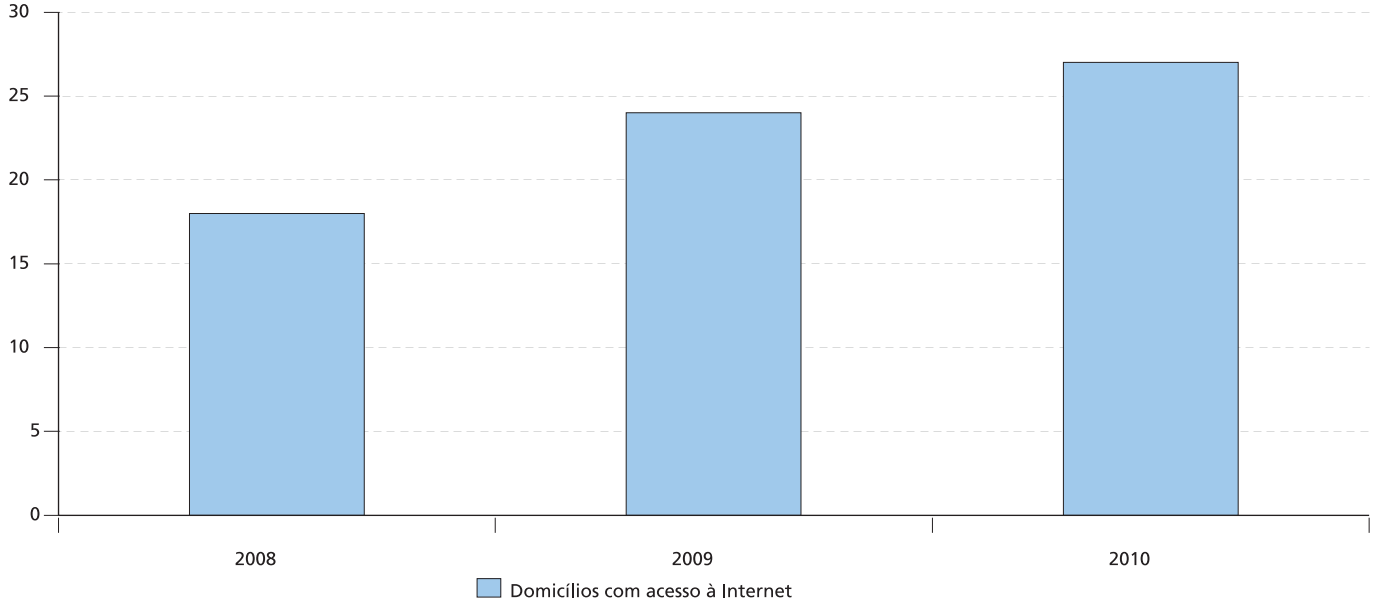
2 DADOS E ANÁLISE

2.1 TIC Domicílios

A principal base de dados utilizada nesta análise provém da Pesquisa Sobre Uso das Tecnologias da Informação e Comunicação no Brasil – TIC Domicílios e Usuários 2010, realizada pelo CGI (CETIC, 2010), cujo objetivo é relatar os desdobramentos contextuais do acesso às TICs. É importante salientar que os dados aqui apresentados são relativos à *identificação* de eventos de segurança e não à efetividade dos problemas relacionados à segurança. A identificação de uma tentativa de invasão difere da constatação de uma invasão, bem como de uma invasão não identificada.

Por meio dos dados da pesquisa, observa-se que os brasileiros estão, gradativamente, ocupando seu lugar no espaço cibernético. Isto pode ser comprovado pelo gráfico 1, que mostra o aumento ano a ano de acesso à internet nos domicílios brasileiros. Quanto maior a quantidade de internautas – o que sugere muita gente novata e inexperiente –, maiores os riscos com a segurança na rede. O governo deve ficar atento a este movimento para conseguir capacitar estas pessoas em termos de segurança na rede.

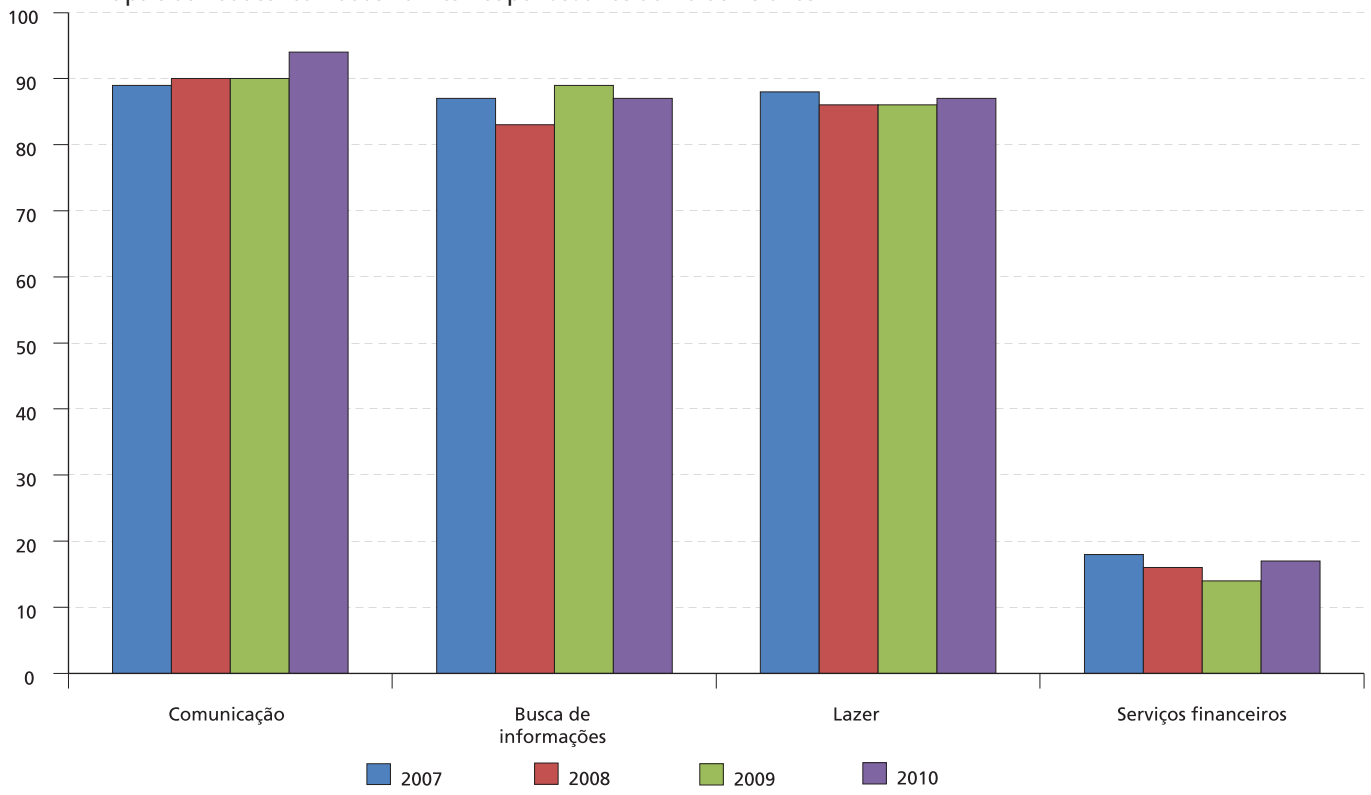
GRÁFICO 1
Porcentagem de domicílios brasileiros com conexão à internet



Fonte: Pesquisa TIC Domicílios e Usuários 2010 (CGI/CETIC).
Elaboração dos autores.

O gráfico 2 destaca uma característica muito peculiar do uso da internet. Nos quatro últimos anos, não houve uma variação muito significativa nos critérios de utilização da rede. Entre as categorias destacadas, a de serviços financeiros é a que menos atrai os internautas durante todo o período em análise.

GRÁFICO 2
Principais atividades realizadas na internet por usuários acima de 18 anos



Fonte: Pesquisa TIC Domicílios e Usuários 2010 (CGI/CETIC).
Elaboração dos autores.

Como as categorias não são excludentes entre si, e considerando-se que o universo amostral é composto por usuários de internet, é possível inferir que o usuário tem a possibilidade e capacidade de usufruir de todas as facilidades e comodidades que a internet pode lhe proporcionar. Entretanto, é observável que parte dos internautas brasileiros não utilizam serviços bancários, mesmo diante da baixa qualidade no atendimento nas agências bancárias e das centenas de campanhas publicitárias empresariais incentivando o uso do *internet banking*.[2]

Se não é pela falta de habilidade no manuseio do computador ou pela falta do instrumento de acesso, é possível que o internauta brasileiro não confie que a infraestrutura de rede lhe garanta total segurança e privacidade ou não está seguro de si mesmo para realizar tais atividades. Incluem-se nessa categoria consultas (conta corrente, poupança, cartão de crédito), transações (pagamentos, investimentos, transferências, DOC, TED, recarga de celular) e outros serviços financeiros.

A pesquisa indicou que 51% dos internautas já realizaram pesquisa de preço na internet antes de adquirir um produto. Apenas 20% deles chegaram a realizar pelo menos uma compra e, destes, apenas 11% relataram ter tido problemas com compras *on-line* (atraso na entrega, produto com defeito, estelionato etc.). Observou-se, ainda, que 29% dos internautas não realizam compras pela internet por preocupação com sua privacidade e segurança. Ou seja, existem vários fatores que impedem a dinamização do comércio eletrônico nacional, tais como falta de segurança na rede e incerteza de punição justa para os usuários de má-fé.

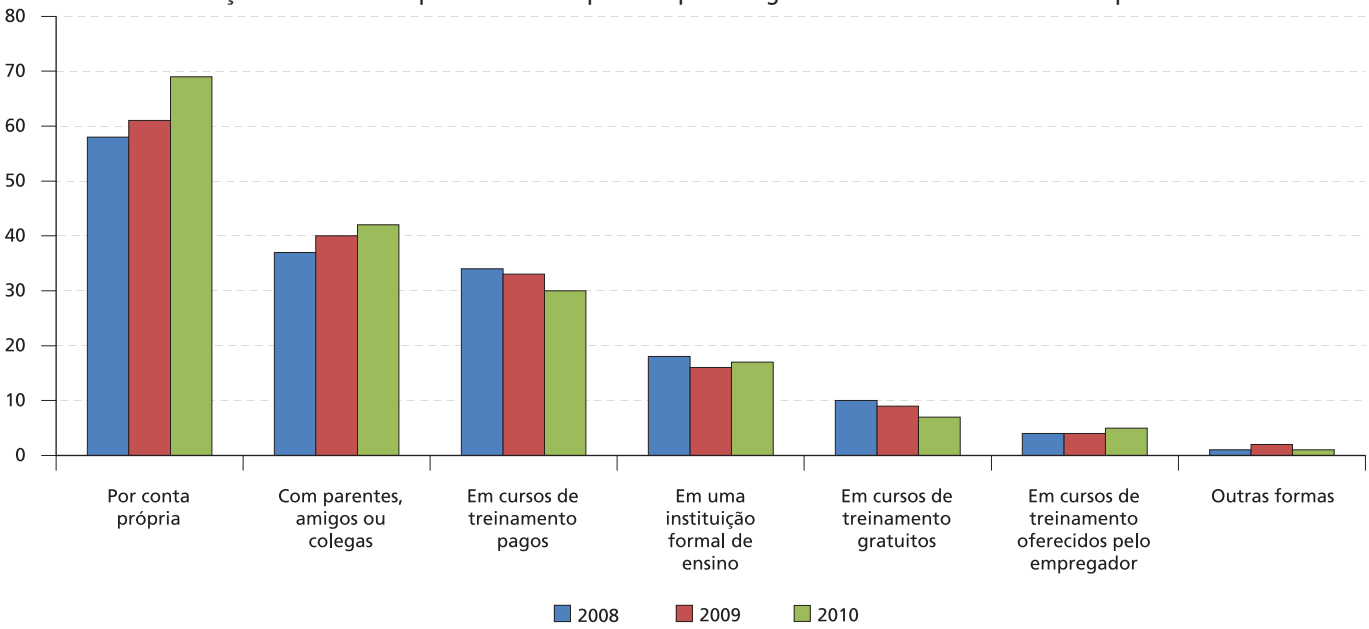
Conforme relatório da Symantec Corporation (2010), o Brasil tornou-se mais proeminente em todas as categorias relacionadas a atividades maliciosas analisadas por ela em 2009, exceto para *spam zombies*, em que já era o país mais bem classificado. Ainda conforme o relatório, o Brasil subiu para a terceira colocação, comparado ao resto do mundo, em atividades maliciosas. Ou seja, o temor dos usuários têm fundamento real. Existem ainda fatores endógenos, por exemplo, no caso em que o usuário não está maduro o suficiente para tomar os cuidados necessários para uma navegação segura. O gráfico 3 mostra uma tendência crescente de usuários que buscam capacitação por conta própria ou

2. É válido ressaltar que esta disparidade na proporção entre o uso de serviços financeiros e atividades como comunicação, lazer e pesquisa é mantida mesmo quando se restringe a amostra para indivíduos com 16 anos ou mais de idade.

com a ajuda de pessoas próximas. Cursos de treinamento e formação estão perdendo espaço entre os novos internautas. Dessa forma, é natural que o processo de aprendizagem se dê de uma maneira não metódica, por meio de tentativas, erros e acertos. Durante este processo, é comum que um internauta novato não tenha acesso facilitado a informações claras, objetivas e seguras sobre segurança cibernética. Elaborar e divulgar documentos explicativos para formação de internautas conscientes pode ser uma boa estratégia governamental, de curto prazo e baixo custo.

GRÁFICO 3

Forma de obtenção de habilidades para uso do computador: percentagem sobre o total usuários de computador



Fonte: Pesquisa TIC Domicílios 2010 (CGI/CETIC).

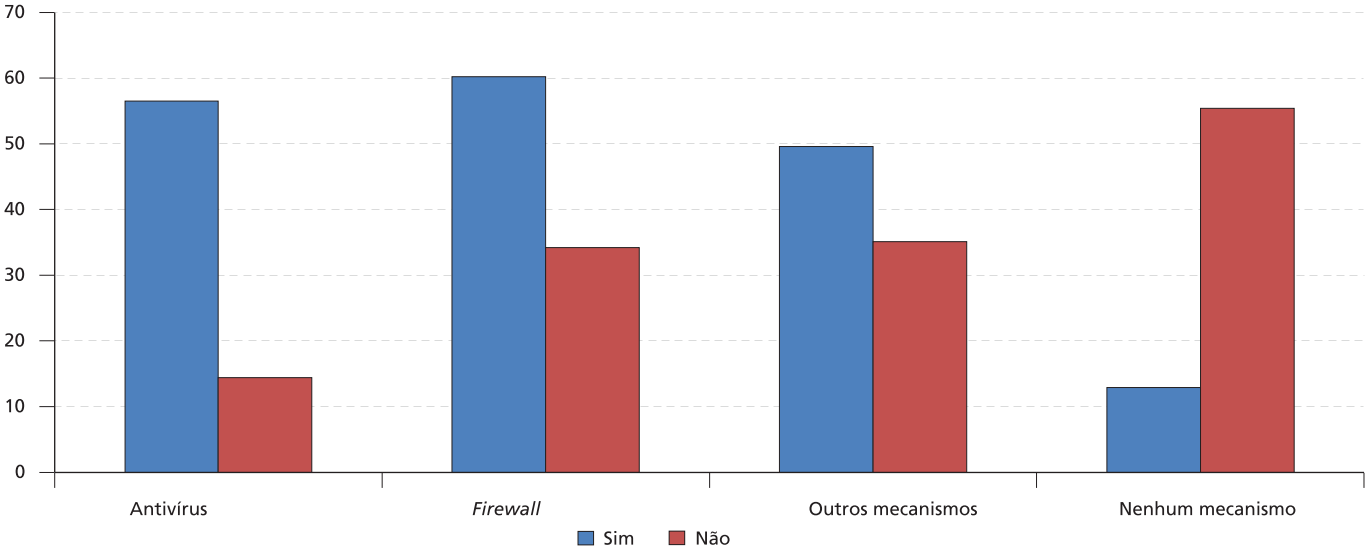
Elaboração dos autores.

Outra evidência que reforça esse argumento é o estudo de Takemura *et al.* (2008), que, por meio de um modelo econométrico, estimado com base numa amostra de firmas provedoras de acesso à internet (PSI) do Japão, aponta que as medidas e ações ligadas à educação e conscientização dos funcionários e usuários apresentam vantagens comparativas na relação custo-efetividade frente aos investimentos ligados à proteção tecnológica.

Por sua vez, os dados do CGI para domicílios apontam a importância de mecanismos tecnológicos no trato com incidentes cibernéticos.

GRÁFICO 4

Proporção de indivíduos que reportaram problemas de segurança – por mecanismo de defesa utilizado



Fonte: Pesquisa TIC Domicílios 2009 (CGI/CETIC).

Elaboração dos autores.

O gráfico 4 revela que há uma maior incidência relativa de problemas de segurança da informação entre indivíduos que reportaram adotar o uso de tecnologias como antivírus, *firewall* ou outros mecanismos como *antispam* e *antispyware*. Isto não significa que os mecanismos de defesa aumentam a probabilidade de ocorrência dos problemas, mas, sim, que há uma maior probabilidade de identificação do problema quando estes mecanismos são empregados.

Em resumo, é importante investir em conjunto tanto em capacitação quanto em tecnologias de segurança, pois ambos contribuem para a segurança do ciberespaço. A seguir, é mostrado que esta também é uma tendência quando se analisam os dados empresariais.

2.2 TIC Empresas

Na abordagem das empresas, a principal base de dados utilizada foi a Pesquisa sobre o Uso das Tecnologias da Informação e Comunicação no Brasil – TIC Empresas 2009, também realizada pelo CGI (CETIC, 2009). Foram elaboradas algumas tabelas, as quais relacionam a incidência de problemas de segurança da informação, a composição de funcionários que acessam a internet na empresa e as medidas de segurança da informação adotadas.

TABELA 1
Estatísticas sumárias – porcentagem sobre o total de firmas com acesso à internet (2009)

	Total	Proporção de funcionários com acesso à internet			
		Até 20%	De 21% a 50%	De 51% a 70%	Acima de 70%
Problema de segurança	**71,6**	65,1	75,7	81,6	81
Vírus	**63**	53,6	65,7	75,9	71
Cavalos de Troia	**53**	44,3	56,3	58,2	60,8
Worms ou *Bots*	**21**	14,9	19,7	29,7	29,4
Acesso interno não autorizado	**9**	7,4	7,9	11,9	11
Acesso externo não autorizado	**9**	5,8	9,7	14,8	13,2
Fraude facilitada por TIC	**6**	5,7	4,4	7,4	9,1
Negação de serviço (DoS)	**5**	3,6	4,9	7,9	8,5
Ataque ao servidor	**5**	3	5,6	5,8	7,6
Departamento de TI - DP.TI	**25**	16,2	25,1	38,4	49,7
Treinamento em TIC	**31**	22,5	32,3	49,4	43
Treinamento em segurança de TI	**38**	27,1	35,3	54,2	59,7

Fonte: Pesquisa TIC Empresas 2009 (CGI/CETIC).
Elaboração dos autores.

O primeiro dado que se pode destacar da tabela 1 é que 71,6%[3] das firmas reportaram ter encontrado algum tipo de problema de segurança. A adoção de contramedidas, tais como uma política de segurança da informação, o treinamento no uso das TICs e a presença de um departamento de tecnologia da informação (TI), é observada em proporções modestas, inferiores a 40% das firmas.

Ao relacionar problemas de segurança com número de funcionários com acesso à internet, percebe-se uma relação positiva entre ambos. De fato, quanto maior a quantidade de funcionários com acesso à rede, mais essa empresa é dependente de tecnologias da informação e maiores também são as possibilidades de falhas. Em outras palavras, utilizando a teoria do elo mais frágil, também conhecida pela expressão em inglês *weakest-link* (VARIAN, 2004), quanto mais elos existirem na cadeia, maior a probabilidade de se ter um elo mais frágil e suscetível à falha.

3. De certa forma essa é uma estimativa otimista, dado que firmas podem omitir a ocorrência de um incidente como forma de preservar a integridade do nome da empresa e o valor da firma perante o mercado.

TABELA 2
Problemas de segurança e existência ou não de departamento de TI e política de segurança

	Contramedidas em segurança da informação			
	Com departamento de TI	Sem departamento de TI	Com política de segurança	Sem política de segurança
Problema de segurança	78,1	69,3	77,8	66,4
Vírus	69,9	58,1	68,5	57
Cavalos de Troia	58,1	48,9	57	48
Worms ou *Bots*	32,3	15,1	29,9	13,7
Acesso interno não autorizado	11,2	7,4	11,1	6,9
Acesso externo não autorizado	14,5	6,5	12,8	6,2
Fraude facilitada por TIC	7,5	5,6	8	5
Negação de serviço (DoS)	8,6	3,8	7,3	3,8
Ataque ao servidor	6,6	4	6,5	3,7
Departamento de TI - DP.TI	-	-	46,9	14,5
Treinamento em TIC	50,4	23,1	49	19,4
Treinamento em segurança de TI	39,5	13,8	44,8	6,5
Política de segurança	65,2	26,5	-	-
Mecanismos de defesa	98,5	95,7	99,4	94,3
Antivírus	98,1	94,6	98,9	93,6
Antispam	84,2	64,8	84,8	61,3
Antispyware	80,8	56,8	79,4	53,7
Firewall	78,4	49,9	77,2	46
Sitema IDS[1]	55	25,2	53,2	21,3
Nenhum	1,5	4,5	0,5	5,7

Fonte: Pesquisa TIC Empresas 2009 (CGI/CETIC).
Elaboração dos autores.

Não obstante, na tabela 2, observa-se que, entre as firmas que possuem um departamento de TI e/ou adotam uma política de segurança da informação, a frequência dos problemas reportados é maior que no estrato de firmas que não possuem política ou departamento de TI. O fato de uma firma reportar um problema de segurança também está ligado à identificação do problema. Empresas que não possuem uma estrutura de TI para controlar e monitorar sua rede podem não conseguir identificar os problemas e vulnerabilidades que possam ocorrer. Portanto, acredita-se que os dados relacionados a empresas com departamento de TI ou com política de segurança sejam mais fidedignos e traduzam melhor a realidade.

Analisando os mecanismos de defesa, ainda na tabela 2, é possível encontrar mais evidências que comprovam a afirmação anterior. Firmas que possuem departamento de TI e/ou política de segurança apresentam melhores mecanismos de defesa em todos seus critérios se comparadas àquelas que não possuem. Por exemplo, a existência de departamento de TI e/ou política de segurança mais do que dobra a chance de a firma contar com um sistema de detecção de intrusão (em inglês, *intrusion detection system* – IDS), que auxilia a identificação de invasões e acessos não autorizados – internos e externos.

Essa análise é condizente com um levantamento feito em 2010 pela Federação Nacional de Varejo dos EUA e pela First Data Corp, que aponta que 64% dos varejistas de pequeno porte acreditam que suas empresas não são vulneráveis a roubos cibernéticos. Embora também não estejam imunes, as empresas de maior porte têm maior capacidade de evitar prejuízos, uma vez que dispõem de maior aporte tecnológico.

Assim como na perspectiva dos domicílios, o investimento em capacitação de pessoas é fundamental para manter toda a estrutura segura. Em todo caso, um dos grandes desafios é convencer a alta administração de que parte dos investimentos deve ser dedicado também a evitar perdas em vez de apenas aumentar os lucros futuros, assegurando, assim, a importância estratégica da segurança cibernética.

3 CONCLUSÃO

Existem duas formas de aumentar a segurança no ambiente cibernético; uma é investir em infraestrutura e tecnologia, e a outra é investir em educação e conscientização do usuário sobre a segurança das informações na rede. O ideal é que ambas sejam desenvolvidas em conjunto, pois, se alguma delas for deixada para trás, fatalmente esta será o elo mais frágil para eventuais problemas de segurança.

Os dados evidenciaram que investimentos em segurança, quer no âmbito tecnológico ou em capacitação, são fundamentais para a identificação de eventos relacionados à segurança. A partir daí, o usuário ou a firma terá condições de escolher a melhor alternativa para eliminar ou minimizar potenciais prejuízos.

Os dados também mostraram que a situação dos indivíduos e firmas no Brasil, em relação a eventos de segurança, não é confortável. Há muito espaço para investimentos e melhorias tanto em sistemas tecnológicos quanto em capacitação de usuários. Elaborar e divulgar documentos para informação e formação de internautas conscientes pode ser uma boa estratégia governamental, de curto prazo e baixo custo, para reduzir a efetividade dos ataques tanto ao cidadão comum como às firmas brasileiras.

Este artigo é o primeiro de uma linha de pesquisa que o Ipea está iniciando para abordar o tema da segurança da informação tanto do ponto de vista privado quanto do setor público.

REFERÊNCIAS

CETIC – CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO. Comitê Gestor da Internet no Brasil. TIC Empresas 2009: pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil. [S.l.]: CETIC, 2009.

CETIC – CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO. Comitê Gestor da Internet no Brasil. TIC domicílios e usuários 2010: pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil. [S.l.]: CETIC, 2010.

MACHLUP, F. **The production and distribution of knowledge in the United States**. Princeton University Press, 1962.

SYMANTEC CORPORATION. **Symantec global internet security threat report**. Apr. 2010. Disponível em: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf>. Acesso em: 5 ago. 2011.

TAKEMURA, T.; OSAJIMA, M.; KAWANO, M. **Empirical analysis on information security countermeasures of Japanese internet service providers**. 2008. p. 18. (Discussion Paper).

VARIAN, H. System reliability and free-riding. *In*: CAMP, L. J.; LEWIS, S. (Eds.). **Economics of information security**: advances in information security. Norwell: Kluwer Academic Publisher, 2004. v. 12, p. 1-15.