# Uma Pesquisa de Segurança da Informação na Região Centro-Sul Fluminense

**Tauller Augusto de Araújo Matos**
USS, Centro de Ciências Exatas, Tecnológicas e da Natureza
tauller@yahoo.com.br

**Maiara Soares Ramos**
USS, Centro de Ciências Exatas, Tecnológicas e da Natureza
maiara_sr@hotmail.com

***Resumo:*** *O valor da informação cresce exponencialmente a cada dia e com isto, o número de ataques virtuais ou digitais tem aumentado consideravelmente. As empresas precisam se preocupar com a segurança, pois os ataques estão cada vez mais sofisticados, porém o investimento em segurança por parte delas não acompanha este crescimento. O objetivo deste trabalho é realizar um levantamento da situação atual das empresas de Vassouras e região Centro-Sul Fluminense com relação à segurança da informação.*

**Palavras-chave:** *Criptografia. Firewall. Proxy. Política de Segurança.*

# A Survey of Information Security in the Central South Fluminense

***Abstract:*** *The value of information grows exponentially every day and with this, the number of virtual or digital attacks has increased considerably. Companies need to worry about security because the attacks are increasingly sophisticated, but the security investment on their part does not accompany this growth. The objective of this study is to survey the current status of Vassouras companies and Fluminense South Central region with respect to information security.*

**Keywords:** *Cryptography. Firewall. Proxy. Security Policy.*

## Introdução

A preocupação com a segurança da informação tem crescido exponencialmente nos últimos tempos. Alguns exemplos de invasão foram noticiados pela mídia recente como sites da Presidência da República, do Portal Brasil, da Receita Federal, da Petrobras, do Ministério do Esporte, do Instituto Brasileiro de Geografia e Estatística (IBGE) e do Ministério da Cultura. Estes ataques têm sido feitos por *Crackers*[1] inspirados no movimento *Anonymous*. O objetivo deste movimento é incentivar a grande massa a lutar pelos seus direitos para poder viver num país com menos desigualdades "Até pouco tempo somente *sites* de empresas ligadas ao governo haviam sido atacados, mas na primeira semana de fevereiro de 2012 o alvo dos ataques foi os *sites* de bancos tanto privados quanto particulares[2-3].

Contudo, os ataques internos conhecidos como *inseder* também são alvos de grande preocupação. O roubo da informação se dá por meio de técnicas de engenharia social com auxilio, às vezes, de funcionários insatisfeitos, e, em alguns casos, são os verdadeiros vilões.

Com isso, surge a grande questão e preocupação: a necessidade de se implementar uma política de segurança da informação nas organizações. Grandes empresas investem milhões em estratégias de segurança e mesmo com este investimento sofrem ataques constantes. Imagine-se o que pode ocorrer com empresa de pequeno porte que não investe em segurança da informação.

O presente artigo é dividido da seguinte forma: na seção 2 são definidos os conceitos de segurança da informação, criptografia *Firewall*, *Proxy* e Política de Segurança. Na seção 3, apresenta-se uma pesquisa realizada em Vassouras e região Sul Fluminense. 50 empresas responderam o questionário. Por fim, na seção 4, é realizada a conclusão, juntamente com as perspectivas deste trabalho.

## Conceitos de Segurança da Informação

A segurança da informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática, a saber, confidencialidade, integridade e disponibilidade (Sêmola, 2003).

*Confidencialidade* – A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas lhe tenham acesso. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas. Exemplo: No Hospital, as fichas dos pacientes só podem ser vista por pessoas autorizadas.

*Disponibilidade* – A informação ou sistema de computador deve estar disponível no momento em que aquela for necessária. Exemplo: no hospital, as fichas dos pacientes devem estar sempre disponíveis.

*Integridade* – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra as alterações indevidas, intencionais ou acidentais. É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas. Exemplo: no hospital, as fichas dos pacientes só podem ser alteradas por pessoas autorizadas.

Outro conceito importante na segurança da informação *é a autenticação*, processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos. Como exemplo podemos citar um usuário que efetua um login de acesso ao computador e/ou sistema.

Sêmola (2003), define segurança da informação, como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, a prática de gestão de riscos de

incidentes que impliquem no comprometimento dos três princípios básicos da segurança: confidencialidade, integridade e disponibilidade da informação. Portanto, as definições das regras que incidiram sobre todos os momentos do ciclo de vida da informação, são: manuseio, armazenamento, transporte e descarte, que viabilizam a identificação e o controle de ameaças e vulnerabilidades.

Para se proteger as empresas devem fazer uso de algumas técnicas para aumentar a segurança da informação.

## Política de Segurança

A informação é um ativo que, como qualquer outro é importante e essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ISO 27002).

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, o que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, o que é necessário para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio (ISO 27002).

Tem-se como vantagem na implementação de uma política de segurança em uma empresa a organização, lembrando que a política não está envolvida apenas com a tecnologia, conforme mencionado, mas engloba todos os ativos. Portanto, com a política pode-se reduzir os riscos e vulnerabilidades (Imoniana, 2005).

## Criptografia

A criptografia tem o objetivo de prevenir fraudes no comércio eletrônico, garantir a validação de transações financeiras, prover a identidade da instituição, proteger o anonimato e prevenir que outras empresas leiam documentos confidenciais. Um processo criptográfico é composto dos seguintes personagens: criptografar, decriptar, emissor e receptor, e por fim o envio e o recebimento da informação.

A criptografia traz uma forma de proteção, como serviços que assegurem confidencialidade, autenticação, integridade para os dados.

Criptografia é o estudo das principais técnicas que transformam a informação original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário. Essa técnica torna a informação ilegível por alguém que não seja autorizado. Sendo assim, só o receptor da mensagem pode ler a informação com facilidade (Kurose, 2010).

Para a proteção dos dados privados são usadas técnicas de criptografia para codificar textos claros em textos desordenados. Quando a mensagem está criptografada torna-se de difícil entendimento por terceiros não autorizados e pode-se atingir o sigilo e integridade da mensagem enviada. O receptor ao detectar a mensagem deverá aplicar o algoritmo de decriptação para ter acesso ao conteúdo.

## Firewall

É uma aplicação que tem por objetivo separar a rede interna da *internet*. Pode ser usado em uma combinação de *hardware* e *software* para obter maiores resultados.

Com sua utilização se tem o controle de todo o tráfego de entrada, saída e redirecionamento dos dados, o que leva o administrador a gerenciar todos os pacotes que passam pela rede e obter maior controle sobre o fluxo de dados.

Com uso de um *firewall* pode-se evitar que um acesso não autorizado obtenha sucesso. Já o uso de um *gateway* (primeiro roteador da rede, máquina onde geralmetne está o *firewall*) bem configurado, pode-se evitar que *sniffers* (programas que coletam dados) possam pegar informações da rede. Com seu uso pode-se combater *malwares* (pragas virtuais que usam portas especificas para explorar vulnerabilidades, e coletar informações) (Neto 2004).

## Proxy

A *internet* está cada vez mais acessível no mundo. Todas as pessoas estão cada vez mais interligadas à rede mundial de computadores. Embora traga vários benefícios, como obter informações em tempo real, *e-commerce*, contato de empresas com seus clientes, há vários problemas que podem ser encontrados. Muitas pessoas passam a maioria do seu tempo navegando por *sites* que não são condizentes pela política da empresa, utilizam a banda da *internet*. De acordo com a Rede Nacional de Ensino e Pesquisa (RNP), 65% da largura de banda das empresas são utilizadas em navegação WEB e esse número tende a crescer cada dia.

Um proxy é uma aplicação que fica entre a rede interna e a internet, geralmente na mesma máquina que o *firewall* (*gateway*), com vários objetivos. Como por exemplo, pode-se efetuar compartilhamento de conexão, *cache* de páginas web, controle de acesso por url, dominio, palavras, usuários. Com a combinação desses e vários outros recursos tende-se a obter um maior desempenho de conexão, respostas de acessos em menor tempo, devido à utilização de *cache*. Com esse controle o administrador pode então ter acesso a todo conteúdo navegado por cada *host* da rede, efetuando filtros por IP ou usuário.

## Pesquisa de Segurança da Informação

Esta seção tem como foco revelar o resultado da pesquisa realizada na região Centro-Sul Fluminense. É uma das regiões político-administrativas do estado do Rio de Janeiro e corresponde à área do Vale do Paraíba, fronteiriça ao estado de Minas Gerais, subdividida nas microrregiões da Vassouras e de Três Rios, ambas cortadas de Oeste para Leste pelo rio Paraíba do Sul. São componentes dessa região os seguintes municípios: Areal, Comendador Levy Gasparian, Engenheiro Paulo de Frontin, Mendes, Miguel Pereira, Paracambi, Paraíba do Sul, Paty do Alferes, Sapucaia, Três Rios e Vassouras.

O objetivo foi buscar e entender como as empresas desta região estão precavendo suas informações e qual conhecimento que têm com relação à segurança da informação. A seguir, são apresentados os resultados desta pesquisa. Os gráficos informam a quantidade de respostas para cada item.

Primeiramente, buscou-se identificar o ramo de atividade das empresas. Observou-se maior concentração nos ramos do comércio varejista e de prestação de serviço, conforme Figura 1. Também foi levantado o número médio de funcionários, Figura 2. Observe-se certo equilíbrio para este item, mas a maior parte concentra-se na faixa de até 50 funcionários.

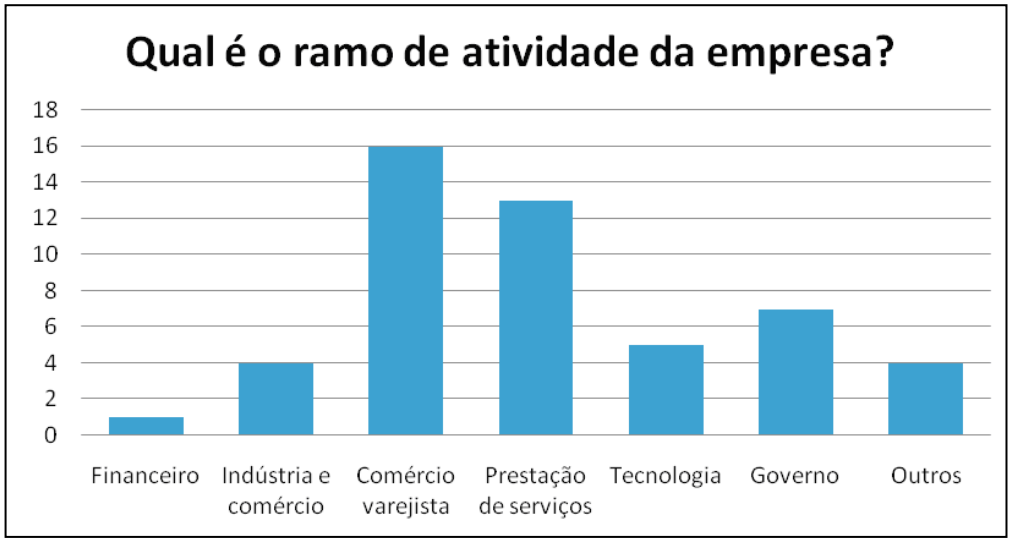


**Figura 1. Ramo de atividade da empresa**

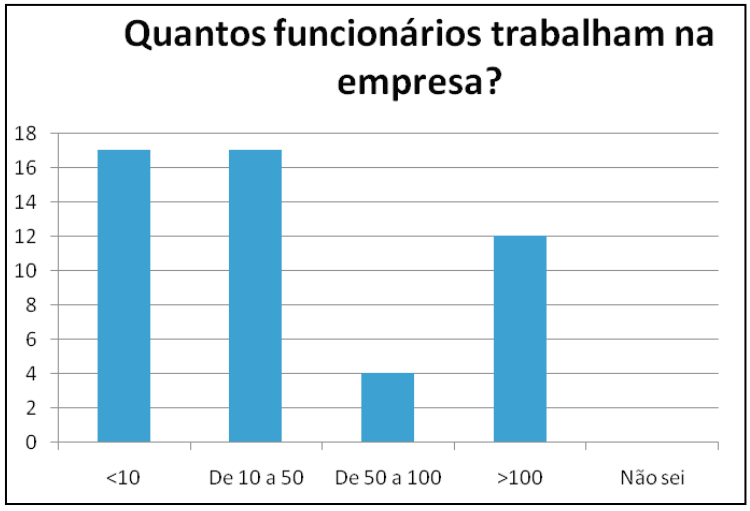


**Figura 2. Quantidades de funcionários na empresa**

As Figuras 3 e 4 são referentes ao departamento de informática e segurança da informação. Observe-se que algumas empresas não têm nenhum funcionário responsável pela segurança da informação, o que representa grande risco.

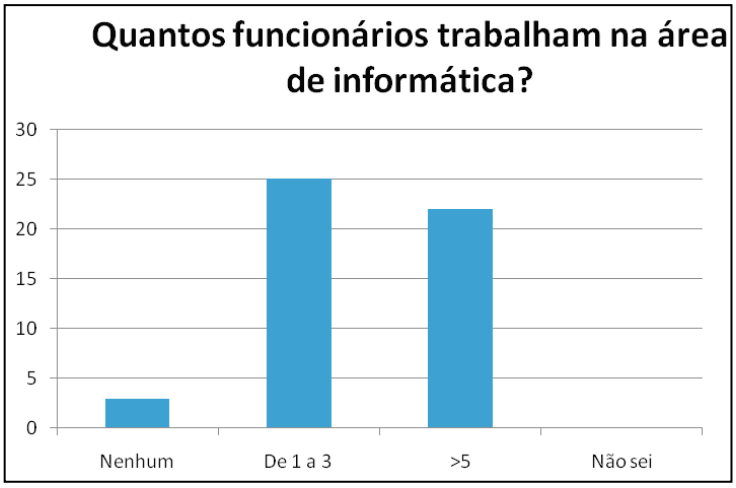


**Figura 3. Quantidade de funcionários na área de informática**

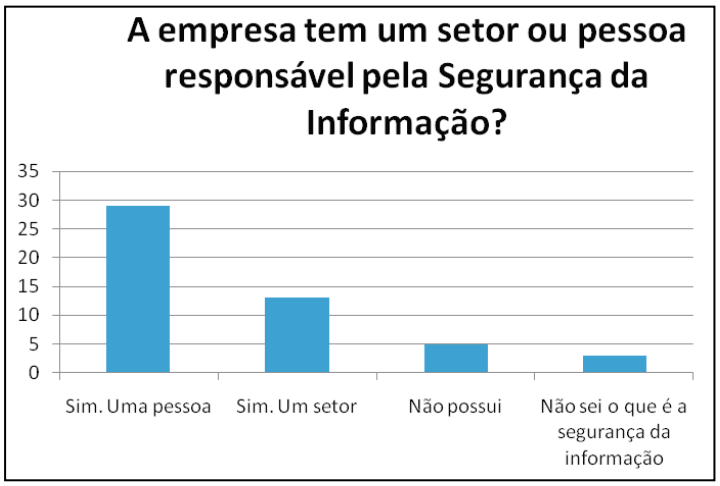


**Figura 4. Relaciona se a empresa tem um setor ou uma pessoa responsável pela segurança de informação.**

Outra questão tratada na pesquisa é a da relação de interesse que a direção da empresa mostra com margem à segurança da informação (Figura 5). Pode-se observar que em 40% dos casos a direção não está interessada, o que pode aumentar e muito os riscos.

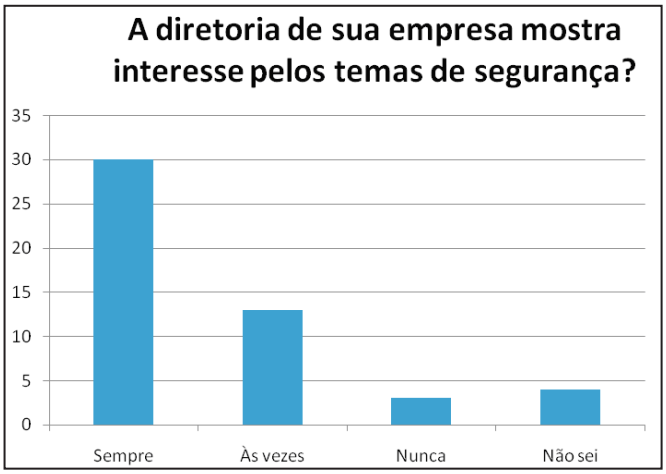


**Figura 5. Interesse da diretoria com relação à segurança da informação.**

Também foi levantado o número de computadores instalados nestas empresas Figura 6. Esta questão é importante, pois quanto maior o número de computadores maior a vulnerabilidade.

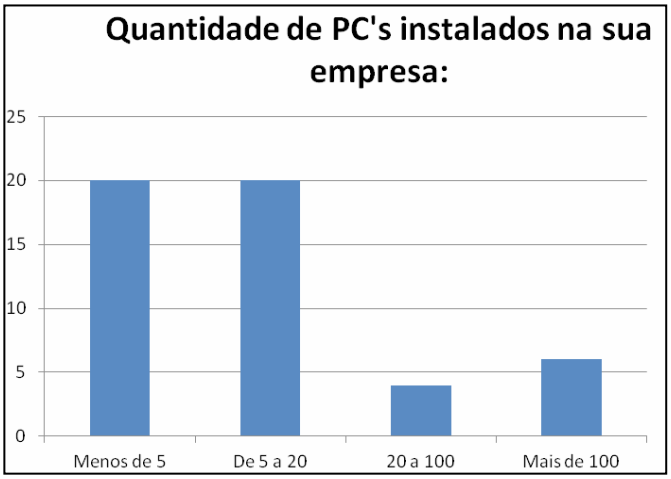


**Figura 6. Quantidade de computadores que as empresas possuem.**

Abordou-se também o sistema operacional utilizado. Conforme Figura 7, grande parte das empresas utiliza o sistema operacional *Windows*. Este sistema, com relação à segurança pode apresentar sérios problemas tais como: i) facilidade de instalação de aplicativos sem licença; hei) acesso fácil ao sistema com perfil de administrador, o que pode resultar na instalação de programas maliciosos, reduzindo assim o nível de segurança. Já sistemas baseados em GNU/Ledos trabalham com uma filosofia diferente, por padrão, o acesso ao modo gráfico é restrito a usuários com perfil limitado, pois não têm permissão de instalar nem executar tarefas administrativas. Com isso, o nível de segurança fica muito elevado. Há de se relatar que qualquer aplicação maliciosa terá dificuldade de infectar um sistema baseado em GNU/ledos.

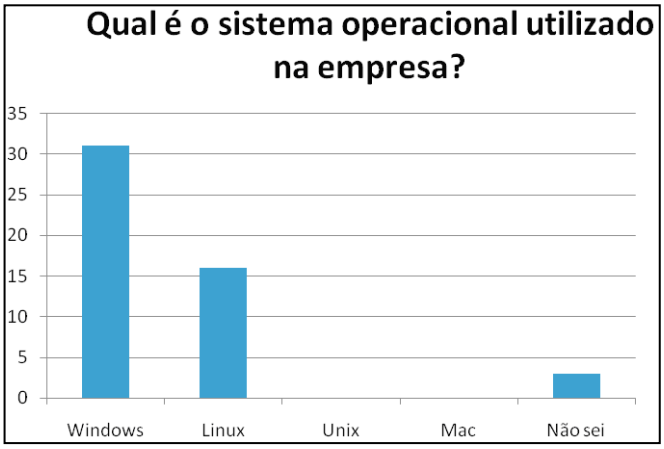


**Figura 7. Resultado do sistema operacional.**

As quatro próximas perguntas se referem às ferramentas utilizadas para aumentar a segurança da informação. Primeiro questionou-se com relação à utilização de antivírus. 90% responderam que fazem uso de antivírus (Figura 8). Destaca-se que para um antivírus ser efetivo precisa ser atualizado, e as máquinas verificadas diariamente. As marcas de antivírus utilizadas podem ser verificadas na Figura 8.1. Todas as empresas utilizam antivírus proprietário, portanto softwares pagos.

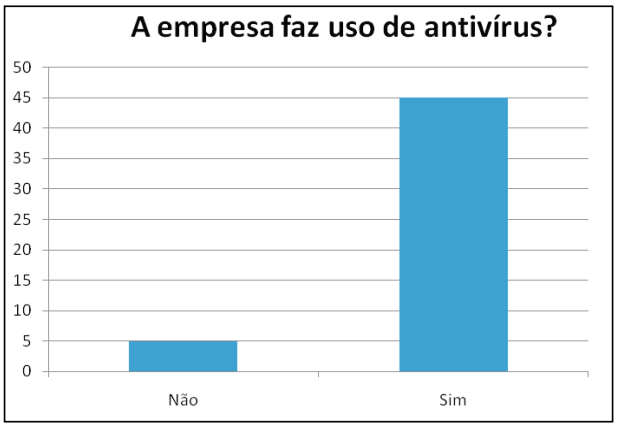


**Figura 8. Utilização de antivírus.**

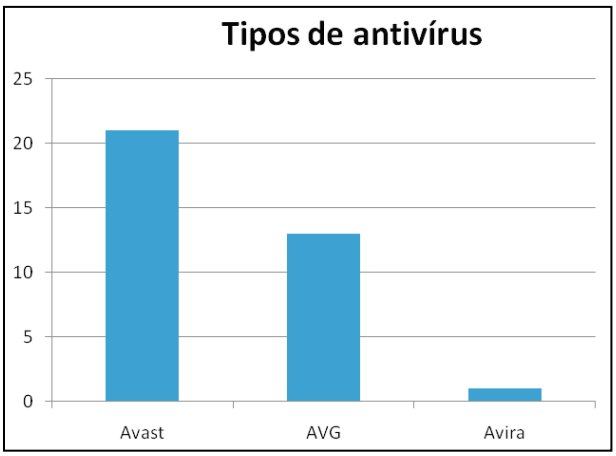


**Figura 8.1. Tipos de antivírus.**

Outro assunto abordado se refere à utilização do *ferial*. Conforme visto anteriormente, o *firewall* é importante, pois impede que a rede ou o computador seja acessado por outra pessoa, sem alteração. As informações que estão na rede ou no computador não podem ser capturadas por ação de *hackers*, pois além de ajudar a combater vírus, têm a capacidade de bloquear as portas que podem ser usadas por "pragas" ou bloquear o acesso de programas não autorizados. As Figuras 9 e 9.1 demonstram que 62% das empresas não utilizam o *firewall*. 23% disseram que utilizam *firewall***.** A maioria utiliza o *firewall* do *Windows*. Este tipo de *firewall* é básico e não garante a segurança em 100%, por este não ser gerenciável nem customizável.

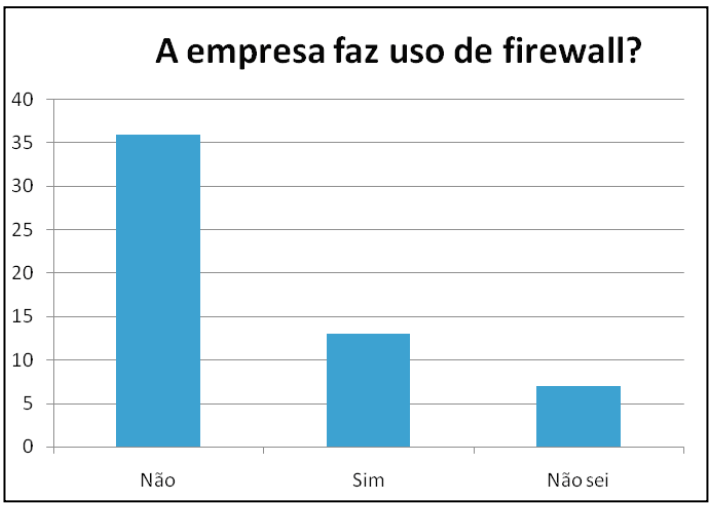


**Figura 9. Uso de *firewall* na empresa.**

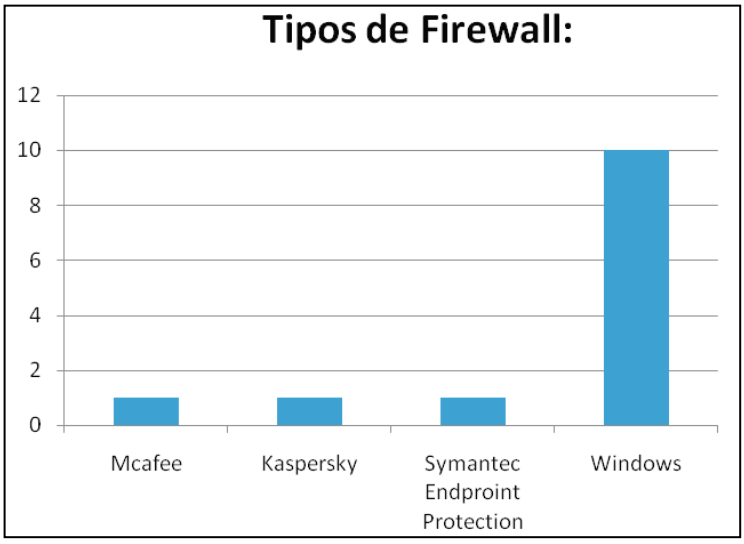


**Figura 9.1. Tipos de firewall.**

Um resultado preocupante tem relação com a adoção da política de segurança. Foi constatado que 95% das empresas não possuem política de segurança (Figura 10). Como mencionada anteriormente, a função da política de segurança é a proteção dos recursos existentes para evitar problemas por meio de normas e procedimentos criados. Quando a empresa não estabelece uma política de segurança, ela tem um grande impacto de falhas nos processos.


**Figura 10. Utilização da política de segurança.**

Conforme visto anteriormente *proxy* é um intermediário entre os computadores de uma rede e a *internet*. Sua função é bloquear o acesso a páginas irrelevantes ao serviço do empregado na empresa. Por exemplo, funcionários que acessam *sites* para fazer *downloads* de músicas, jogos etc. Esses acontecimentos prejudicam o rendimento das empresas. A Figura 11 relata que 62% das empresas fazem uso de *Proxy*.

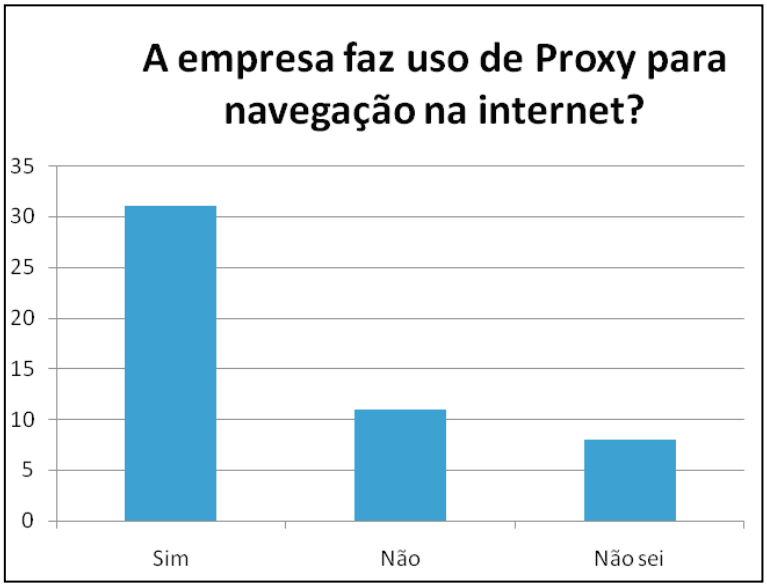


**Figura 11. Utilização de *Proxy*.**

Questionamos também se a empresa possui controle de acesso aos setores. Este controle de acesso pode ser físico ou lógico. O acesso físico refere-se às instalações, já o segundo, diz respeito ao acesso aos computadores. Conforme Figura 12, 60% das empresas têm controle de acesso aos setores, mas 40% ainda não apresentam controle em todos os setores.

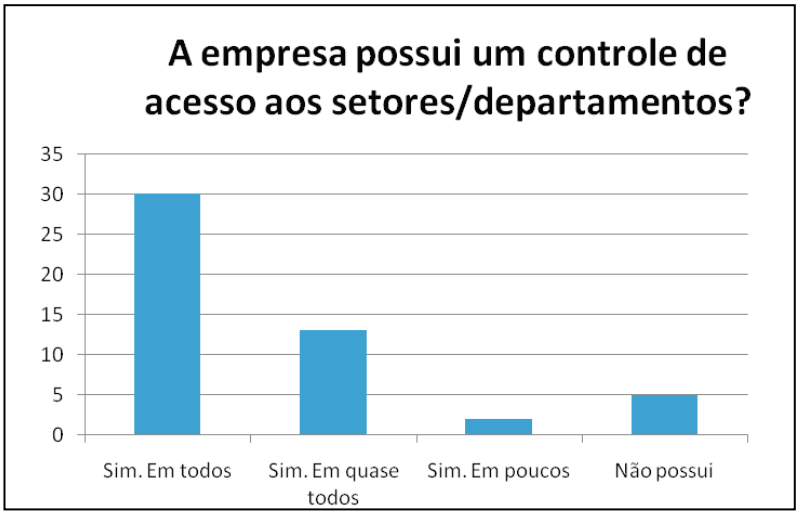


**Figura 12. Controle de acesso aos setores.**

Para finalizar, verificou-se que 70% (Figura 13) das empresas utilizam autenticação de acesso aos computadores (*login)*. Neste caso, não basta apenas ter autenticação nos computadores. Caso o usuário tenha permissão de administrador, poderá realizar todas as atividades como instalar *softwares* e alterar configurações da máquina. Isto não é viável. É necessário ser feita uma autenticação com o perfil do cargo do funcionário. Com isto, surge a importância da senha para que futuras auditórias sejam realizadas.

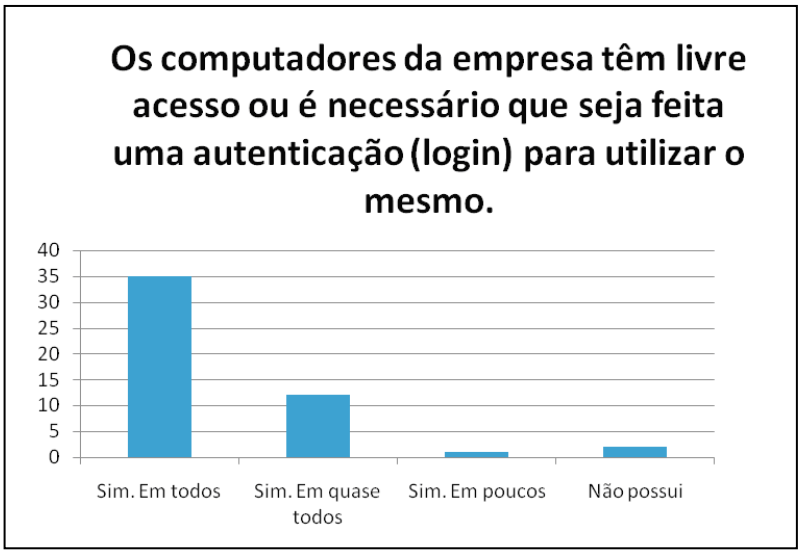


**Figura 13. Autenticação para utilizar os computadores**

## Conclusão

Não há como impedir o roubo de informações por meio de redes de computadores em 100%. Mas é possível a prevenção e a diminuição do risco, se utilizadas as técnicas de segurança da informação. As técnicas de invasões e roubos aumentam gradativamente, por isto, é necessário que o setor de segurança da empresa evolua juntamente com estas técnicas.

Este trabalho teve como objetivo pesquisar como as empresas da região Sul Fluminense estão investindo na segurança da informação e o quanto podem ser vulneráveis a ataques de *hackers*. O resultado da pesquisa demonstra que as empresas não estão dando a devida importância à segurança da informação. Muitas empresas veem esse empreendimento como gasto, e não investimento.

Como trabalho futuro pretende-se aumentar o número de empresas participantes do questionário e o número de questões, e por fim, ministrar palestras educativas para mostrar a importância da segurança da informação para estas empresas.

## Notas

1 Invadem sistemas para roubar e danificar informações.

2 http://www.istoe.com.br/reportagens/143548_2 brasil+sob+ataque+de+hackers

3 http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html

## Referências

Imoniana, Joshua Onome (2005). *"Auditoria de Sistemas de Informação"*. 1.ª ed. São Paulo: Atlas.

ISO 27002. *"Introduction To ISO 27002 (ISO27002)"* Endereço: http://www.27000.org/iso-27002.htm, Acesso em 22/02/2012.

Kurose, James F. (2010). "*Redes de Computadores e a Internet: Uma Abordagem Top-Down"*. 5. ª ed. São Paulo: Pearson.

Neto, Urubatan (2004). *"Dominando Linux Firewall IPTables"***.** Editora: Ciência Moderna. 1.ª edição.

Sêmola, Marcos (2003). "*Gestão da Segurança da Informação: Uma Visão Executiva"*. Rio de Janeiro: Campus.

Disponível em: http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html. Acesso em 15/03/2011

Disponível em: http://www.istoe.com.br/reportagens/143548brasil+sob+ataque+de+hackers. Acesso em 15/03/2011.