A Methodology for Integration of Technologies and Procedures for Security of Information

Ranieri Marinho de Souza (Faculdade de Engenharia Elétrica, PUC-Campinas, Brasil) ranieri.marinho@gmail.com
Alberto Lotito (Faculdade de Engenharia Elétrica, PUC-Campinas, Brasil) alotito@gmail.com
Marcelo Aparecido Morales (Faculdade de Engenharia Elétrica, PUC-Campinas, Brasil) marcelo.morales@kaizen.com.br
Eric Alberto de Melo Fagotto (Faculdade de Engenharia Elétrica, PUC-Campinas, Brasil) eric.amf@uol.com.br

In this work we present the first results obtained through the use of a methodology that we are developing for integration of technologies and procedures for security of information in an organization environment. Such methodology will permit the implementation of NBR ISO/IEC 17799 and NBR ISO/IEC 27001 standards through the use of hardware and software technologies nowadays available. Our results refer to the monitored vulnerabilities of a corporate network through the use of an intrusion detection software and of the adopted policies to eliminate them.
Keywords: Security, Technology, Information, NBR ISO/IEC 17799 and NBR ISO/IEC 27001.

Uma Metodologia para a Integração de Tecnologias e Procedimentos para a Segurança da Informação

Neste trabalho apresentamos os primeiros resultados obtidos com uma metodologia que estamos desenvolvendo para a integração de tecnologias e procedimentos para a segurança da informação em um meio organizacional. Esta metodologia permitirá a implantação das normas NBR ISO/IEC 17799 e NBR ISO/IEC 27001, mediante a utilização de tecnologias de hardware e software disponíveis atualmente. Nossos resultados referem-se ao monitoramento de vulnerabilidades em uma rede empresarial, mediante o uso de um software para a detecção de intrusos e as políticas a serem adotadas para eliminá-las.

Palavras chave: Segurança, Tecnologia, Informação, NBR ISO/IEC 17799 e NBR ISO/IEC 27001.

1 Introdução

Devido aos constantes avanços tecnológicos e a larga utilização de sistemas de informação, a cada dia que passa, a segurança torna-se um dos temas mais relevantes para gestores de Tecnologia da Informação (TI) e demais responsáveis nas organizações. Um verdadeiro arsenal de regulamentações, metodologias e certificações associadas a uma grande variedade de ferramentas de *hardware*, *software* e sistemas de prevenção está em permanente desenvolvimento para poder suprir as necessidades de segurança.

O maior reflexo disso é o lançamento de novas normas, como a NBR ISO/IEC 17799 [1] e NBR ISO/IEC 27001 [2] que foram criadas para estabelecer diretrizes e princípios para melhorar a gestão de segurança nas organizações. A publicação dessas normas demonstra a importância conquistada pela segurança da informação, que passa a ser percebida como estratégica para o negócio de qualquer companhia, envolvendo fatores importantes como à imagem que as organizações possuem junto aos seus parceiros, por exemplo, aos clientes e fornecedores.

A importância da implantação das normas em conformidade com as necessidades em uma organização aponta para o desenvolvimento de políticas e aplicação de recursos de *hardware* e *software* que suportem a segurança da informação. Contudo, a publicação de novas normas não está relacionada diretamente ao desenvolvimento de *hardware* e *software*. Assim, a existência de diversas normas e técnicas de segurança não é usualmente implantada de modo integrado e depende fortemente da iniciativa de cada empresa. Em vista disso, é corriqueiro que tal procedimento não solucione o problema da segurança da informação e somente acarrete uma maior burocracia e complexidade no tratamento das informações dentro das empresas [3]. Colocado isto, podemos dizer que muitas ferramentas podem ser utilizadas de maneira inadequada, como por exemplo, o *firewall* para a defesa de redes de computadores. Sua utilização isolada não resolve completamente os problemas das redes, que ainda são vulneráveis a outras formas de ameaças, tais como ataques via *SQL Injection* [4].

Neste trabalho apresentamos os primeiros resultados de uma metodologia que estamos desenvolvendo para integração entre tecnologias e procedimentos para segurança da informação. O objetivo dessa metodologia é o de educar, prevenir e finalmente detectar, quando não for possível impedir ataques e invasões a redes de computadores. Ressaltamos que nossa proposta visa uma implementação das normas NBR ISO/IEC 17799 e NBR ISO/IEC 27001, mas é importante se ter claro que tais normas dizem o que deve ser feito e não como deve ser feito.

Este artigo está organizado nas seguintes seções: Introdução, Políticas de segurança, Escolha das ferramentas, Escolha das tecnologias e considerações finais. Todos os testes foram realizados na empresa Tecnicopias Gráfica e Editora Ltda no período compreendido entre julho de 2006 e janeiro de 2007.

2. Políticas de Segurança

Para implantar políticas de segurança devemos seguir uma sistemática que requer cuidados em sua aplicação, pois envolverá a organização de uma empresa como um todo, além de influenciar diretamente seus clientes, fornecedores e colaboradores.

Começamos por estabelecer uma comissão para a criação e desenvolvimento do sistema de gestão de segurança da informação (SGSI). Após isso, devemos entender as normas e suas implicações, bem como o que consideraremos como itens de segurança para somente então levarmos a discussão a todos os setores, utilizando como intermediadores os departamentos de Recursos Humanos (RH) e de Tecnologia da Informação (TI). Após o estabelecimento do SGSI, são realizados todos os treinamentos necessários com os colaboradores, clientes e fornecedores. Com os treinamentos concluídos, passamos a avaliação da eficácia por intermédio de auditorias e após isso partimos para a certificação NBR ISO/IEC 27001 por uma consultoria competente. Se não for obtida a certificação, devemos desenvolver um plano de ação refazendo os treinamentos e passar por uma nova auditoria para obter a certificação. É importante salientar que a certificação é algo opcional, ficando isso a critério da própria empresa.

O plano acima parece simples de ser colocado em pratica, porém existem diversos fatores políticos e técnicos que dificultam sua implantação. Esses fatores devem ser resolvidos junto à direção da organização, pois são estes os maiores interessados e os que detêm o poder necessário para patrocinar as políticas que devem ser colocadas em prática. A nível de direção, a questão da segurança é vista como fator de garantia da imagem da empresa perante seus clientes e fornecedores, além de assegurar que as informações da empresa não serão utilizadas para fins impróprios como, por exemplo, espionagem industrial.

Podemos observar que uma política de segurança consiste em especificar formalmente as regras que deverão ser seguidas pelos colaboradores e demais interessados para acessarem e manipularem os recursos de informação da empresa. Sempre devemos tomar como base as normas NBR ISO/IEC 17799 e NBR ISO/IEC 27001, porém adequadas à realidade de cada organização.

Para a execução e implantação das normas é sugerida uma atuação baseada no modelo PDCA (*Plan-Do-Check-Act*) [2], que é esquematicamente representado na Figura 1 do ciclo PDCA.

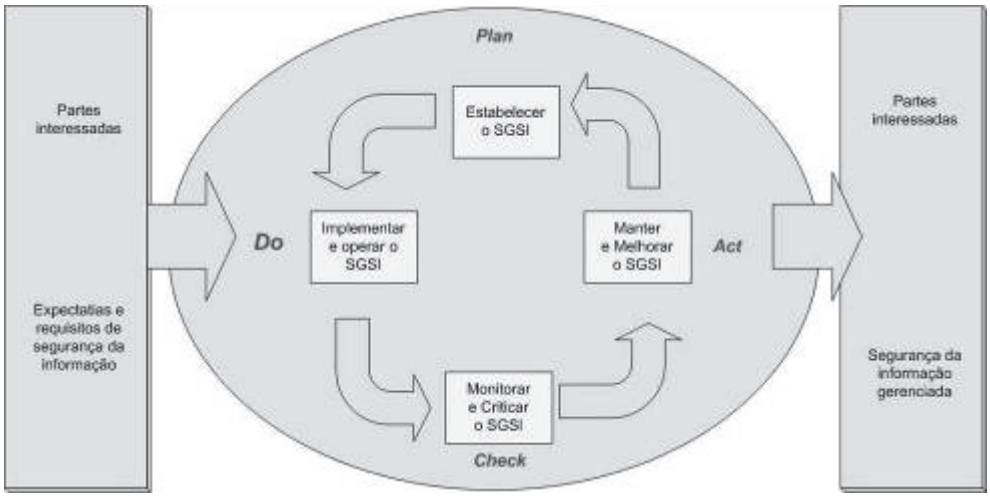

Figura 1 – Ciclo PDCA conforme [2]

Na empresa Tecnicópias identificamos que as informações que necessitam de segurança são todas aquelas que possuem dados referentes a transações com clientes, fornecedores e colaboradores. As transações antes eram realizadas através do envio e recebimento de correio eletrônico (*e-mail*) e arquivos em mídia magnética ou ótica, sem controle efetivo do transporte e da divulgação de seu conteúdo. Após a implantação e divulgação da política de segurança, toda comunicação e transporte de dados foi normatizada com o treinamento e controle de acesso a dados da rede e também o controle de acesso a locais restritos, já que antes todos os funcionários poderiam circular livremente entre os setores da empresa.

O envio de arquivos e informações por *e-mail* está sendo monitorado. O envio de arquivos é realizado apenas através do servidor de FTP (*File transfer protocol)* aliado a uma página de serviços que possui um controle efetuado através do envio de protocolos aos interessados. Tais protocolos permitem verificar tanto dados como datas de envio e de alteração dentre outros, ficando proibido o envio e recebimento através de *email* ou de mídia magnética ou ótica. O compromisso dos clientes, fornecedores e colaboradores com esta regra simples reduziu em muito o atraso nos trabalhos.

Medidas tomadas durante testes realizados na empresa Tecnicópias, mostraram que o envio de *emails* com arquivos anexados de tamanhos variando entre 10 Mb e 20 Mb resultavam em até 2 horas de espera, estas decorridas desde o envio do arquivo até a sua recepção mediante o uso do protocolo SMTP (*Simple mail transfer protocol*) do *software* de *e-mail*.

Outra regra simples adotada foi o controle de acesso, realizado mediante utilização de travas nas portas e portões dos setores que possuem acesso restrito, restringindo assim o acesso aos departamentos que trabalham com informações críticas tais como salários e arquivos de clientes dentre outros.

3. Escolha das ferramentas

A escolha das ferramentas é facilitada depois de se adotar as políticas de segurança, pois nesse ponto já conhecemos as informações que devemos controlar e quais os níveis de acesso que cada usuário e setor da empresa deve possuir. Apresentamos na figura 2 o diagrama de redes da empresa Tecnicópias que utilizamos como base de teste para este trabalho.

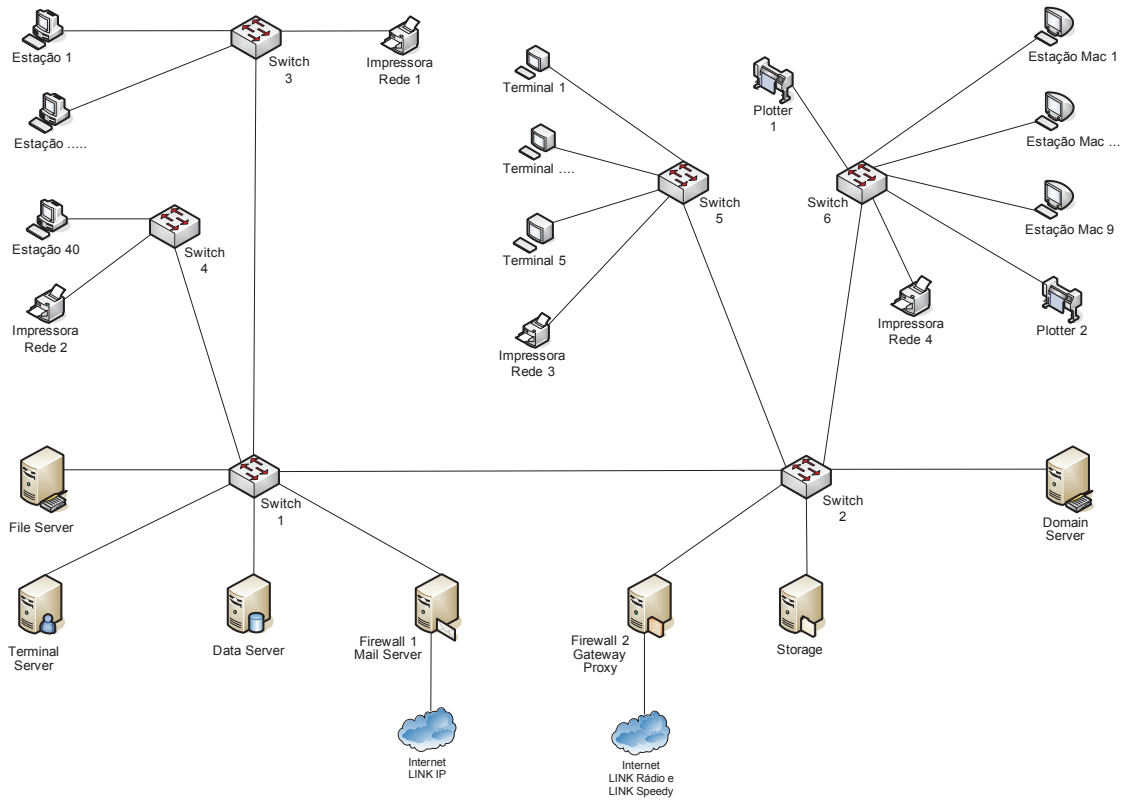

Figura 2: Infra-estrutura de redes da empresa Tecnicópias Gráfica e Editora Ltda. (utilizada com permissão da empresa).

3.1 Escolha das tecnologias

Após análise da infra-estrutura apresentada na figura 2, podemos buscar os *softwares* necessários à aplicação das políticas de segurança estabelecidas pelo SGSI.

3.1.1 Utilização de *Freeware* (software livre)

A primeira medida foi a adoção de *freeware*, uma escolha importante que pode trazer benefícios de custos, não necessitando disponibilizar recursos para sua aquisição. Dessa forma, possibilitando o desenvolvimento das ferramentas de acordo com as necessidades da empresa que adotará o sistema. Porém não descartamos aqui a possibilidade da utilização de ferramentas comerciais por outras empresas.

Até o momento foram testadas as ferramentas Snort (Sistema de detecção de intrusão) e Ethereal (varredura de portas), que se mostraram eficientes na geração de alertas, históricos e análise de dados.

3.1.2 IDS (Sistema de detecção de intrusos)

O IDS é um sistema de detecção de intrusos freqüentemente utilizado em conjunto com um firewall, que possibilita o envio de alertas ao administrador de redes através da configuração de assinaturas e regras de acesso. Além disso, possui um controle ativo que, ao contrário do firewall, verifica os pacotes e os compara com as assinaturas, negando o acesso ao código malicioso. O *software* IDS escolhido foi o Snort, que é um *software* livre para detecção de intrusão a redes, desenvolvido inicialmente por Martin Roesch [5], capaz de desenvolver uma análise de tráfego em tempo real e registro de pacotes em redes IP. Através dele se faz análises de protocolo, buscas/associações de padrões de conteúdo e ainda pode ser usado para se detectar uma variedade de ataques, tais como: *buffer overflow* (estouro de pilha ou transbordamento de dados), *stealth port scans* (ataque a portas de redes TCP e UDP), ataques CGI (estouro de pilha ou transbordamento de dados), *Exploit* (seqüência de comandos que se aproveita das vulnerabilidades de um sistema), ataques a *Netbios* (pacotes procedentes do mundo exterior visando compartilhamentos em sistemas operacionais Windows), P2P (*softwares* de compartilhamento de arquivos), dentre outras. Essa ferramenta é suportada em arquiteturas RISC e CISC e em plataformas das mais diversas, como nas várias distribuições de Linux e também na plataforma Windows.

Mediante os resultados apresentados na figura 3 observamos que é necessária a utilização de um IDS para se possuir um sistema de alerta e negação de acesso ativo, já que o *firewall* Linux (*Iptables*) é um controle passivo que depende de configurações fixas e que por sua natureza não emite alertas.

Podemos verificar que a customização das regras do *firewall* e a utilização dos alertas do Snort permitiram administrar melhor a segurança da informação, porém não devemos nos esquecer de instalar e atualizar o *software* antivírus e manter os programas aplicativos e sistemas operacionais na sua última versão.

Um fato importante é que após a análise pudemos entender que um dos servidores de rede (servidor de FTP) possuía um serviço ativo que colaborava para acrescentar ao alerta do Snort muitas leituras de *Web-IIS* (servidor de páginas). Isso demonstra que os administradores de redes necessitam de ferramentas que possibilitem uma análise mais acurada do tráfego na rede e suas possíveis vulnerabilidades. Existem vários servidores e portas ativas na rede que diversas vezes não executam nenhuma tarefa importante, mas que contribuem para a quebra de segurança, facilitando os ataques dos mais diversos tipos. Algo que preocupa são os ataques aos servidores de banco de dados SQL, que é um tema de pesquisa da maioria dos *Hackers* e que não são satisfatoriamente protegidos apenas com *firewall*.

Na figura 3 podemos identificar muitas ocorrências de Ping, porém essas não representam risco se as portas dos servidores e os compartilhamentos possuem segurança. Quanto ao Netbios (serviço de compartilhamento de pastas e impressoras), foi verificado que algumas estações da rede possuíam serviço de compartilhamento desnecessário e por isso foram reconfiguradas para sanar esta vulnerabilidade.

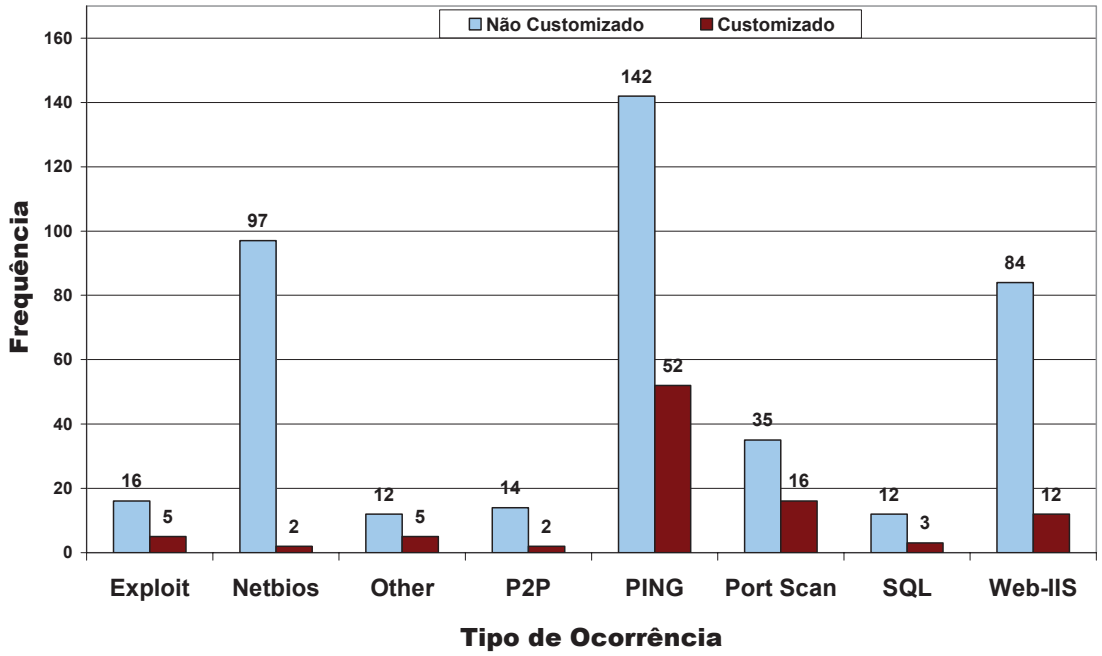

Figura 3 – Ocorrências do sistema não customizado em comparação ao sistema customizado

Na figura 4 apresentamos um exemplo de configuração utilizando o Snort (indicado por IDS 1 e IDS 2). Este software IDS deve ser instalado em uma máquina ligada a um *Hub* em modo promíscuo (i.e., capturando todos os pacotes, independentemente de serem ou não destinados a ele), pois se o conectarmos a um *Switch,* não vamos poder coletar todos os alertas de maneira satisfatória, visto que somente iremos capturar dados da rede local (LAN). Porém, poderíamos utilizar *Switchs* com capacidade de espelhamento de portas e assim não haveria a necessidade da utilização de *Hub.*

Para a configuração das assinaturas e das regras de acesso do Snort, foi levado em consideração os serviços proporcionados pelos servidores da rede como: compartilhamento de pastas e impressoras, FTP, *WEB-IIS* e banco de dados SQL.

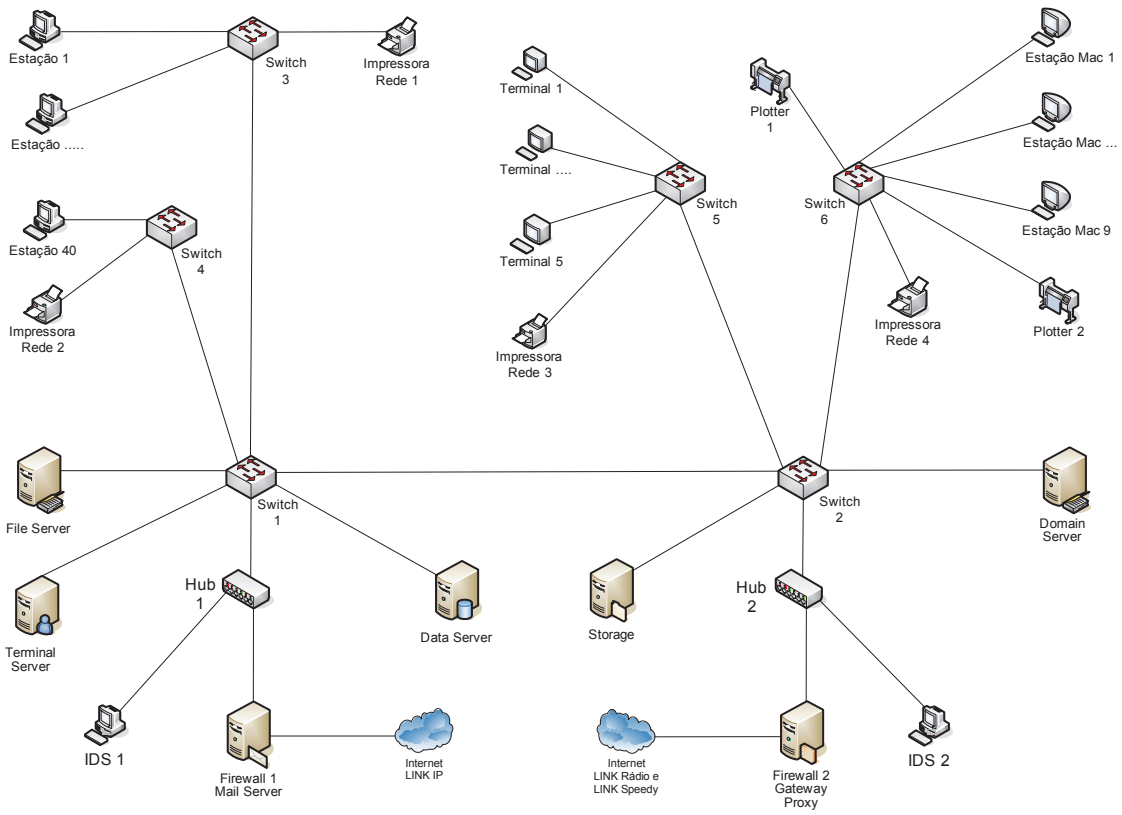

Figura 4 – Infra-estrutura de redes com IDS na empresa Tecnicópias Gráfica e Editora Ltda.

4. Considerações finais

Neste trabalho apresentamos os primeiros resultados referentes à implementação de uma metodologia que estamos desenvolvendo, que utiliza a integração de tecnologias para garantir a segurança da informação em um ambiente organizacional. A partir do monitoramento do fluxo de rede realizado com o auxílio de um software de detecção de intrusos, o Snort, foi possível descobrir vulnerabilidades na rede de uma empresa. De posse dessas informações, o *firewall* foi reconfigurado e tais vulnerabilidades praticamente eliminadas. Este é um trabalho em andamento e para completarmos a implementação da metolodologia que estamos propondo, será ainda necessário cuidarmos da segurança no que se refere ao manuseio de dados, (proteção contra revelação e política de licença), à realização de *backups*: (*backup* de *softwares*, arquivamento dos *backups* e destruição de dados), à propriedade intelectual (atribuição de *copyright*, e proteção do direito autoral), à resposta a incidentes (notificação de incidentes, determinação dos responsáveis, definir o que é notificado e regras jurídicas) e à utilização de criptografia de dados (a ser empregada em contratos firmados com clientes/fornecedores e sistemas de validação)

Entendemos que a totalidade da nossa solução se valerá de tecnologias e procedimentos já existentes para obtermos o controle efetivo de transações envolvendo informações confidenciais. Esperamos que nossa metodologia contribua para preencher uma lacuna existente entre as normas e as ferramentas de software voltadas à segurança da informação. Podemos tomar como exemplo os requisitos das normas NBR ISO/IEC 17799 e NBR ISO/IEC 27001 que são: i) políticas de segurança da informação, organizando a segurança da informação que depende do desenvolvimento das políticas, gestão de ativos, ii) segurança em recursos humanos, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acessos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, gestão da continuidade do negócio e conformidade.

Finalmente, queremos agradecer à Tecnicópias Gráfica e Editora Ltda pela utilização de sua infra-estrutura para a realização dos testes e a cessão dos resultados que apresentamos neste trabalho.

Referências

[1] Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 17799:2005 – Código de prática para a Gestão da Segurança da Informação, 2005, p.1-128.

[2] Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 27001:2006 – Sistemas de Gestão de Segurança da Informação - Requisito, 2006, p.1-42.

[3] MÓDULO Security Solution. 2006. Disponível em: http://www.modulo.com.br. Acesso em: 18 dez. 2006.

[4] C. Peikari and A. Chuvakin. Security Warrior - Know Your Enemy. O'Reilly, 2004, p. 1-552.

[5] M. Roesch. Snort Users Manual – The Snort Project. Sourcefire Inc, 2006, p. 1-131.