Integrando a Segurança da Informação a um Sistema de Gestão Organizacional

Tema: Otras técnicas/temas emergentes en el campo de la Gestión de la Innovación.

Categoria: Trabajo acadêmico

Celso Alberto Saibel Santos
Universidade Salvador - Unifacs
E-mail: saibel@unifacs.br

Alaíde Barbosa Martins
Cetrel S.a.
E-mail: alaide@cetrel.com.br

Resumo:
A Segurança da Informação tem despertado um grande interesse nos últimos anos, pela presença crescente dos sistemas computacionais em rede no nosso cotidiano. Apesar disso, pouco esforço tem sido dedicado à especificação de diretrizes, processos e técnicas que auxiliem a implantação de um Sistema de Gestão da Segurança da Informação (SGSI) em um ambiente em rede. Visando suprir esta deficiência, este trabalho tem como principal contribuição a apresentação de uma metodologia de referência para a concepção, elaboração e implantação de um SGSI em uma organização. Outra contribuição importante do trabalho é a proposta de integração entre os controles, processos e passos de sistemas de gestão baseados nas normas ISO 9001, ISO 14001 e OHSAS 18001 com a norma ISO/IEC 17799, específica de segurança da informação. A integração entre estas normas facilita a implantação dos controles e o aproveitamento das estruturas de gestão existentes, reduzindo o tempo de implantação do SGSI e favorecendo o envolvimento e participação dos colaboradores da organização.

Palavras-chave: Segurança da Informação, ISO 17799, Gestão de Segurança da Informação, Sistema Integrado de Gestão.

1 Introdução

Apesar da diversidade de trabalhos relacionados ao tema Segurança da Informação, pouco enfoque tem sido dado à definição de uma metodologia ou mesmo, de um conjunto de diretrizes consistentes e coerentes, que auxiliem o planejamento e a implantação de um Sistema de Gestão da Segurança da Informação (SGSI)[1] em um ambiente de rede com sistemas computacionais heterogêneos. Visando suprir esta deficiência, este artigo propõe uma metodologia teórico-conceitual para auxiliar a concepção, elaboração e implantação de um SGSI em uma organização, a qual está baseada numa série de normas internacionais, dentre as quais, (TECSEC, 1985), (ISO 15408:1999), (ISO/IEC TR 13335:1998), (BS7799-2:2001), (ISO/IEC 17799:2001) e (IEC 61508:1998). A metodologia apresenta aspectos gerenciais de condução na implantação do SGSI e sua aplicação resulta na padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas, além da criação de indicadores, registros e da definição de um processo educacional de conscientização da organização envolvida.

Uma outra contribuição importante do artigo é a proposta de integração da norma ISO/IEC 17799 (específica de segurança da informação) e as normas e padrões associados a um Sistema de Gestão Integrado, envolvendo as normas ISO 9001 (qualidade de produtos ou serviços), ISO 14001 (meio-ambiente) e OHSAS 18001 (saúde e segurança ocupacional). Esta integração permite a reutilização de uma série de controles, processos e passos tipicamente adotados nestas três últimas normas aos controles da ISO/IEC 17799 para a implantação do SGSI organizacional, além de facilitar o processo de auditoria combinado destas normas.

O artigo está organizado em 6 seções após esta parte introdutória. A seção 2 discute as linhas gerais do processo de implantação de um SGSI organizacional. A seção seguinte apresenta uma proposta de metodologia para nortear a implantação de um SGSI. A seção 4 mostra como é possível adicionar controles relativos à segurança, aproveitando-se das ferramentas de gestão e controle já implementados num Sistema de Gestão Integrado. A seção 5 apresenta a metodologia utilizada para o desenvolvimento do trabalho. Finalmente, na seção 6 são apresentadas as conclusões do trabalho e uma análise da aplicação dos conceitos propostos neste trabalho no ambiente organizacional da empresa Cetrel S.A. – Empresa de Proteção Ambiental.

2 O Processo de Implantação da Segurança da Informação

A preocupação com a segurança dos sistemas computacionais não é recente. O processo de definição de regras e padrões de segurança iniciou-se na década de 60 (com o impulso da Guerra Fria), culminando com a publicação, no final do ano de 2000, da norma Internacional de Segurança da Informação ISO/IEC-17799, a qual possui uma versão aplicada aos países de língua portuguesa, denominada (NBR ISO/IEC-17799:2001).

A norma ISO/IEC 17799 surgiu num momento em que as organizações de todo o mundo passaram a investir muito mais em segurança da informação, muitas vezes sem orientação. Devido à sua notoriedade, a norma ISO 17799 passou a ser referenciada como sinônimo de segurança da informação. Porém, a idéia de que a implantação da segurança da informação em uma organização se resume à verificação de alguns controles sugeridos pela norma ISO/IEC 17799 é um grande mal entendido. A norma contempla ao todo 127 controles, porém nem sempre é necessária a adoção de todos estes mecanismos para se atingir o patamar de segurança desejado. Isto exige uma seleção criteriosa dos controles a partir da realização de uma análise de risco.

[1] Em inglês ISMS (*Information Security Management System*)

Além disso, é necessária a integração de outros padrões e normas (algumas vezes menos conhecidos), mas que podem ser de grande importância na gestão de segurança da informação em uma determinada organização. Como exemplo, podem ser destacados a norma (ISO/IEC TR 13335:1998) e o padrão (IEC 61508:1998). A análise detalhada destes padrões e normas permite a identificação da superposição dos seus controles e da complementaridade de vários dos seus aspectos. Assim, a implantação da gestão de segurança da informação começa pela definição de quais dos itens especificados em cada padrão ou norma devem ser implementados ou seja, se estes itens são ou não adequados às características da organização em questão.

O processo de construção do Sistema de Gestão de Segurança da Informação (SGSI) que é proposto neste trabalho está baseado no modelo de implantação e gestão descrito na (BS7799-2:2001) e na cláusula 7 da (ISO/IEC TR 13335-2:1998).

A norma BS 7799-2 norma oferece as ferramentas para a implantação e gestão através do modelo PDCA (*Plan-Do-Check-Act*). Neste modelo, as fases *Plan-Do* do PDCA correspondem às etapas de construção do SGSI envolvendo a elaboração da política de segurança, definição do escopo, desenvolvimento da análise de riscos, formalização da estratégia de gestão de riscos, documentação e seleção dos controles aplicáveis para reduzir os riscos quando necessário. Assim, a implantação do SGSI se dá efetivamente nas duas primeiras fases do primeiro ciclo PDCA. Ainda no ciclo do modelo PDCA, as fases *Check-Act* estão relacionadas à verificação de que as medidas de segurança especificadas estão sendo aplicadas, às soluções de segurança utilizadas e à melhoria contínua do conjunto de segurança, além das auditorias periódicas de cada componente do sistema.

O sucesso de um Sistema de Gestão Integrado, incluindo a gestão de Segurança da Informação, deve também garantir que uma das mais importantes recomendações da ISO 13335-2 está sendo aplicada. Em suma, deve ser acordado que os representantes de todos os setores da organização estão comprometidos com a política de Segurança da Informação a ser implantada. Este comprometimento é obtido através da criação de um comitê ou fórum de segurança da informação, que deve se encontrar regularmente para balizar e respaldar o trabalho do chamado *Security Officer*[2]. Uma das funções principais deste comitê é definir o nível de risco aceitável pela organização. Dependendo do tamanho da organização, além deste comitê, é recomendada a criação de um departamento de segurança da informação, sob responsabilidade do *Security Officer*. Algumas organizações podem ter também uma diretoria de segurança que engloba as áreas de segurança física ou patrimonial e segurança lógica. Seja qual for o modelo usado, é indispensável que o *Security Officer* tenha visibilidade em toda a organização. A inexistência do comitê provavelmente afastará o departamento de segurança das decisões estratégicas, fazendo com que este se torne um departamento meramente operacional da área de Tecnologia da Informação.

3 Metodologia de Implantação de um SGSI

Cabe deixar claro que elaborar uma metodologia de implementação para o projeto de segurança da informação é uma tarefa complexa devido ao detalhamento que inclui todos os tópicos, itens e aspectos, tanto os técnicos quanto os de caráter gerencial, portanto estar completamente fora do escopo deste artigo detalhes técnicos para atender às

[2] O *Security Officer* é a pessoa responsável pela aplicação ou administração da política de segurança aplicada ao sistema (RFC2828, 2000).

necessidades específicas de cada organização. Porém com um esforço adicional de detalhamento, a metodologia poderia vir a se tornar uma referência para implantação e acompanhamento de Sistemas de Gestão da Segurança da Informação em organizações. A figura 1 apresenta a metodologia proposta através de uma seqüência de passos e dos resultados (*deliverables*) produzidos a cada etapa. Os passos da metodologia, seus resultados e as normas a eles associados são apresentados a seguir.

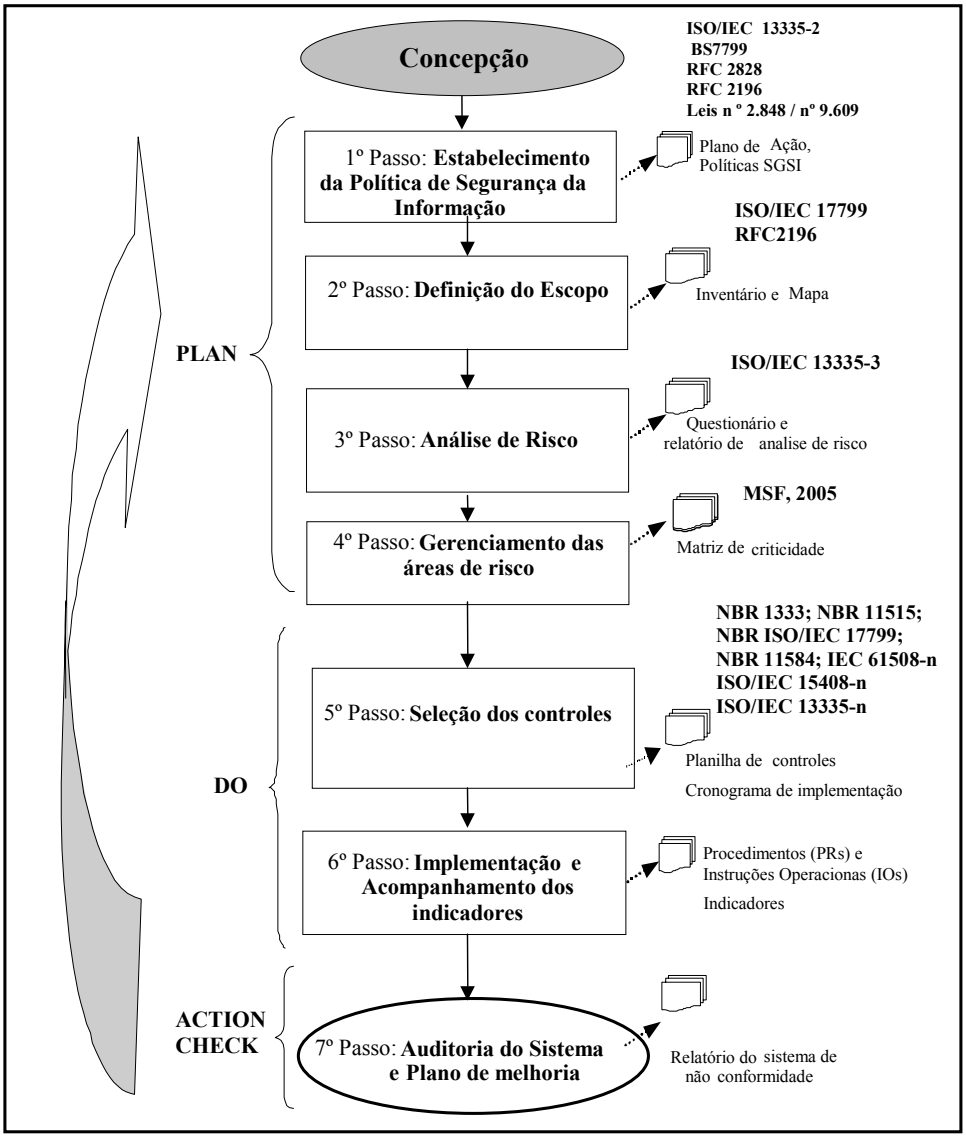


Figura 1 – Metodologia para Implantação de um SGSI.

3.1 A Concepção do Sistema

A etapa inicial, que ocorre antes da realização do primeiro passo da metodologia, corresponde à etapa de **concepção** do sistema. É neste momento em que se determina a viabilidade do projeto, realiza-se o planejamento inicial de suas fases, bem como algumas estimativas iniciais de custo, alocação de pessoal, cronograma, escopo, objetivos e metas. A etapa de concepção pode ser dividida em duas fases. Na primeira, é feito um diagnóstico da situação atual da organização no que diz respeito à

política de Segurança da Informação e a possibilidade de aproveitamento de alguns controles já implementados. Na segunda, faz-se o planejamento do sistema e preparação para a sua implantação. Conforme as normas ISO/IEC TR 13335-2 e BS7799, é nesta fase que deve ser formado o comitê responsável pela implantação do SGSI na organização. Este comitê deve realizar a formação básica e a conscientização dos colaboradores, o planejamento e a preparação do sistema, o detalhamento do projeto e a definição/consolidação da política de segurança e finalmente, estabelecer objetivos e metas para o Programa de Gerenciamento da Segurança da Informação, de acordo com o planejamento estratégico da organização.

3.2 Estabelecimento da Política de Segurança da Informação

A construção da política de segurança é função do comitê formado na etapa de concepção e deve estar baseada nas normas BS7799/ISO17799 e nas *RFC's* de número 2196 (1997) e 2828 (2000). O conjunto de leis que dispõem sobre os crimes cometidos no campo da informática e suas penalidades (Decreto Lei n ° 2.848, de 07 de dezembro de 1940) e sobre direitos autorais e propriedade de software (Lei n° 9.610/98, de 19 de fevereiro de 1998) devem ser utilizadas como referência nesta etapa.

Conforme as *RFC's* 2196 e 2828, a política de segurança é um documento que deve descrever as recomendações, as regras, as responsabilidades e as práticas de segurança. Entretanto, a política de segurança deve ser moldada às especificidades de cada organização, isto é, não existe uma "política de segurança modelo" que possa ser implementada em todo e qualquer caso. Assim, elaborar uma política de segurança é uma tarefa complexa e que necessita ser constantemente monitorada, revisada e atualizada.

A norma ISO/IEC17799 define uma série de características a serem apresentadas pela política de segurança. Segundo a norma, a política deve: (i) ser aprovada pela diretoria, divulgada e publicada de forma ampla para todos os colaboradores; (ii) ser revisada regularmente, com garantia de que, em caso de alteração, ela seja revista; (iii) estar em conformidade com a legislação e cláusulas contratuais; (iv) definir as responsabilidades gerais e específicas; (v) dispor as conseqüências das violações.

Além destas características a política de segurança deverá abranger os seguintes tópicos:

- Propriedade da Informação – é importante determinar o responsável por uma informação, o qual poderá definir quem tem direito de acesso às informações e em que nível, e qual a periodicidade necessária para a cópia (*backup*) desta informação.
- Classificação da informação – o responsável deve classificar a informação quantos aos princípios de disponibilidade, confidencialidade e integridade.
- Controle de acesso – deve atender ao princípio de menor privilégio. Todo pedido de acesso deve ser documentado e as trilhas de auditoria devem ser armazenadas.
- Gerência de Usuários e Senhas – as senhas devem ser únicas e individuais, seguindo critérios de qualidade (isto é, senhas fortes com trocas periódicas). A responsabilidade da senha é de seu proprietário.
- Segurança Física – os acessos a áreas de risco devem ser consentidos mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas, recomendando-se a criação de normatizações de controles internos referentes à segurança física, os quais devem ser auditados periodicamente.

- Desenvolvimento ou compra de sistemas/software – é importante definir uma sistemática interna para isto com ênfase nos requisitos de segurança.
- Plano de continuidade de negócios – é um dos mais importantes tópicos da política, sendo recomendada a geração de controles e padrões especificando detalhes quanto ao plano de contingência e continuidade dos negócios.

Além das características mencionadas, vale ressaltar que as políticas criadas devem ser seguidas por todos os colaboradores da empresa e devem servir como referência e guia de segurança da informação. Para isto, é necessária a realização de uma campanha de divulgação e conscientização de sua importância para a organização.

3.3 Definição do Escopo

A definição do escopo inclui o levantamento dos ativos que serão envolvidos, tais como: Equipamentos; sistemas; nome da organização; estrutura de comunicação (Internet, correio eletrônico); pessoas; serviços; infra-estrutura de rede e classificação da informação.
À medida que evolui, o projeto deve ser revisado e detalhado. Esta revisão é baseada no escopo do projeto, pois a declaração do escopo é um documento que contém a base para as futuras decisões. A delimitação do escopo é extremamente necessária, pois quanto maior o escopo maior a complexidade do SGSI a ser implementado.
O passo 2 da metodologia proposta produz como resultados, o mapa do perímetro da rede de computadores onde será aplicado o SGSI, além do inventário e a classificação dos ativos. A realização do inventário dos ativos da rede (hardware e software) geralmente utiliza ferramentas computacionais específicas, tais como, a ferramenta gratuita MSIA – *Microsoft Software Inventory Analyzer* (MSIA, 2005) – voltada ao levantamento de softwares do ambiente Windows e a ferramenta recomendada pela *Business Software Alliance* (BSA), denominada *Tally Systems WebCensus Service* (TALLY, 2005).

3.4 Análise de Risco

No passo 3 é realizado o diagnóstico da segurança para o escopo definido, através da identificação dos ativos de informação envolvidos e do mapeamento de todas as ameaças relacionadas a estes (COBRA, 2002). Para cada ameaça deve ser determinado o nível de risco envolvido. No desenvolvimento da análise de riscos, a ISO 13335-3 ocupa um papel importante, pois esta norma trata detalhadamente a questão dos riscos, apresentando diversas opções e estratégias de condução da análise de riscos que podem ser escolhidas em função do tempo e orçamento existente e dos objetivos. Após esta fase, o uso da BS 7799-2 na atividade de decidir a estratégia de gestão de riscos é de grande utilidade.
Após o diagnóstico dos riscos, deve-se definir junto à alta administração da empresa, quais os níveis de risco aceitáveis e não-aceitáveis. Entre os não aceitáveis, pode-se escolher uma entre as seguintes opções: (i) reduzir o nível de risco (com a aplicação de controles de segurança); (ii) aceitar o risco (considerar que ele existe, mas não aplicar qualquer controle); (iii) transferir o risco (repassar a responsabilidade de

segurança a um terceiro, como, por exemplo, um *data center*) e por fim; (iv) n  egar o risco.

A análise de riscos pode ser tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada em *know-how* e geralmente realizada por especialistas. Não é possível afirmar com certeza qual é a melhor abordagem, uma vez que cada uma delas fornece uma ferramenta valiosa para a estruturação das atividades de identificação de riscos.

A abordagem quantitativa se baseia nas informações coletadas no processo qualitativo. Novamente, ferramentas computacionais específicas para computar os dados de análise de risco podem ser de grande utilidade nesta fase. Dentre outras, podem ser destacadas a Precision Tree, da Paragon (PrecisionTree, 2005) e a Microsoft Solutions Framework, da Microsoft (MSF, 2005).

Devido à sua agilidade, geralmente as empresas tendem a adotar o modelo qualitativo, que não requer cálculos complexos. Independente do método adotado, uma análise de riscos deve geralmente contemplar atividades como o levantamento dos ativos, a definição de uma lista de ameaças e a identificação de vulnerabilidades nos ativos. O relatório de análise de risco deve apresentar: (i) a identificação e a classificação dos ativos e processos de negócio; (ii) a análise de ameaças e vulnerabilidades; (iii) a análise e parametrização dos riscos e (iv) a definição de tratamento dos riscos.

3.5 Gerenciamento das Áreas de Risco

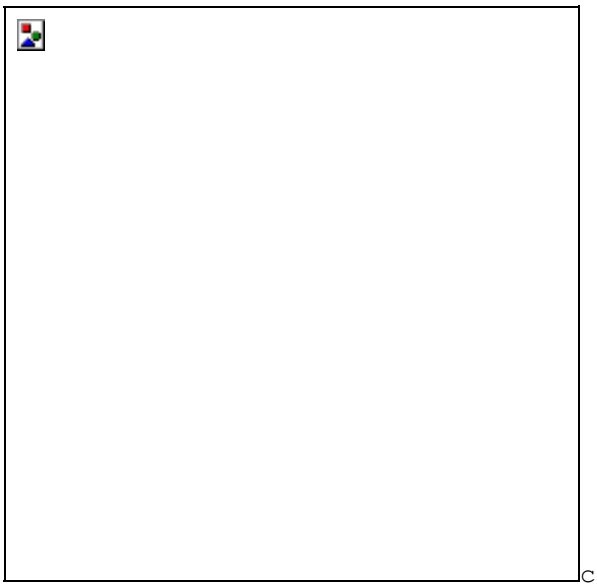
O Gerenciamento de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes. Neste passo é estimado o impacto que um determinado risco pode causar ao negócio. Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança. Uma vez que os riscos tenham sido identificados e a organização definiu quais serão tratados, as medidas de segurança devem ser de fato implementadas. Ainda neste passo, podem ser definidas medidas adicionais de segurança, como os Planos de Continuidade dos Negócios – que visam manter em funcionamento os serviços de missão-crítica, essenciais ao negócio da empresa, em situações emergenciais – e *Response Teams* – que possibilitam a detecção e

avaliação dos riscos em tempo real, permitindo que as providências cabíveis sejam tomadas rapidamente.
Deve-se buscar implantar a gestão pró-ativa dos riscos, que envolve um conjunto de etapas pré-definidas que devem ser seguidas para impedir ataques antes que eles ocorram. Essas etapas incluem verificar como um ataque poderia afetar ou danificar o sistema de computador e quais as suas vulnerabilidades. O conhecimento obtido nessas avaliações pode ajudar a implementar diretivas de segurança que vão controlar ou minimizar os ataques.
Seguir estas etapas para analisar cada tipo de ataque resultará em um benefício indireto: começará a surgir um padrão dos fatores comuns a diferentes ataques. Esse padrão pode ser útil para determinar as áreas de vulnerabilidade que representam o maior risco para a empresa.
Como pode ser notado, este passo está totalmente associado ao passo anterior e, portanto, deve-se ter sempre em mente a necessidade de equilibrar o custo da perda de dados e o custo da implementação dos controles de segurança.

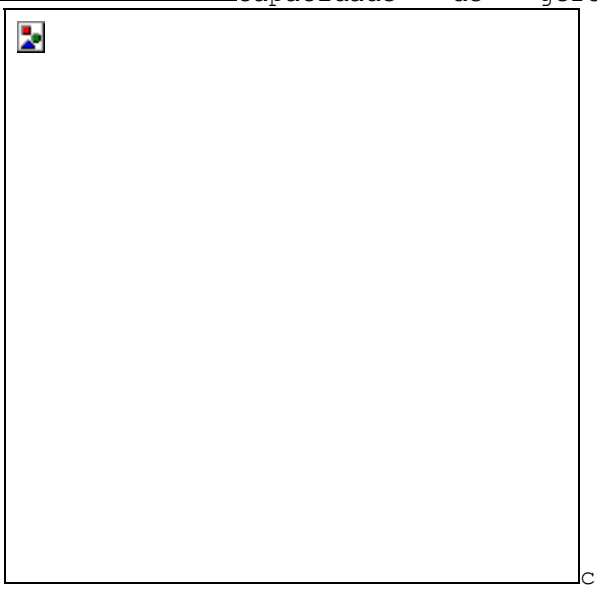
3.6 Seleção dos Controles e Declaração de Aplicabilidade

Após a identificação dos requisitos de segurança, convêm que os controles sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Dentre os 127 controles da BS7799-2 são selecionados, aqueles são aplicáveis à gestão de segurança da informação. Deve-se ainda observar os controles contidos nas demais normas e técnicas existentes para que estes possam ser integrados de forma natural ao SGSI (como proposto anteriormente).
Não basta instituir uma série de regras a serem cumpridas internamente. Para garantir a segurança de uma empresa, é necessário estabelecer procedimentos e controles para o acesso de parceiros externos à corporação, como por exemplo: definição de critérios para acesso às bases corporativas e da política de uso da intranet e Internet; definição de modelo de identificação de pirataria; de gerenciamento de rede; de distribuição de versões de software e de padrões Internet; detecção de inatividade de *modems* ligados à rede; definição do padrão de atualização de antivírus e do acesso de empregados ao provedor corporativo; padronização do portal institucional e do *site* comercial; implantação, roteamento, criptografia, certificação digital, configuração de *firewall*, dentre outras ferramentas e tecnologias necessárias.
Após levantamento dos controles, devem ser realizadas a análise e seleção dos mesmos. Neste caso, recomenda-se utilizar um formulário de declaração de aplicabilidade. Com base nesta declaração, os procedimentos normativos devem ser gerados ou simplesmente revisados de acordo com o sistema normativo já existente na organização.

Entre os critérios para a seleção de controles devem ser considerados: a relação custo x benefício; a aplicação do mesmo controle para reduzir outros níveis de risco considerados não aceitáveis; a



capacidade de gerenciamento do



controle e a capacidade de substituição do controle.

Após sua definição, os controles devem ser implementados dentro do escopo estabelecido, seguindo as informações geradas durante o processo de análise de riscos, tomando o cuidado de sempre manter o foco nos propósitos do negócio, evitando prejudicar, inviabilizando ou retardando demasiadamente, a atividade fim da organização.

3.7 Implementação e Acompanhamento dos Indicadores

Os processos de implantação de contramedidas e de diretivas de segurança ocorrem durante toda a fase de implantação da metodologia. Em seguida, deve ocorrer um processo de acompanhamento de todos os controles implementados e, para isso, é necessária a produção de indicadores específicos que possibilitem visualizar as condições de funcionamento e desempenho do ambiente analisado.

A implementação dos controles selecionados pode envolver a aquisição de tecnologia de software e/ou hardware (custos adicionais), mas em alguns casos, essa implementação resulta apenas na criação de padrões e normas internas a serem obedecidas.

3.8 Auditoria do Sistema

As auditorias internas do SGSI têm a finalidade de verificar, com base em evidências objetivas, se as seguintes condições ocorrem satisfatoriamente:

a. Os procedimentos e instruções operacionais são adequados e eficazes.
b. Os setores da Empresa vêm atuando em concordância com os documentos normativos.
c. Os subsídios fornecidos são suficientes para elaboração dos relatórios periódicos de análise crítica do SGSI.

Para que as auditorias internas ocorram com eficácia, recomenda-se que alguns princípios sejam seguidos, como por exemplo, a independência dos auditores, o planejamento e notificação prévios, o aprimoramento contínuo do SGSI e a busca de constatações e observações que agreguem valores às atividades referentes à segurança da informação, aos objetivos e metas da organização e às suas políticas.

As não conformidades (reais e potenciais) detectadas no SGSI devem ser registradas de acordo com procedimento específico, incluindo ações para registro e tomada de ação para encerramento da mesma. É indicada uma análise crítica destas não conformidades e, se pertinente, é executada a investigação de suas causas, a definição e a implantação de ações corretivas e o registro das alterações em procedimentos. Após a implantação das ações corretivas, deve ser feita uma avaliação de sua eficácia antes de seu encerramento.

Não conformidades potenciais são detectadas através do relato de incidentes relacionados ao SGSI, através da identificação de situações de riscos e da análise detalhada de modificações ou implantação de novas atividades e equipamentos. Uma vez detectadas as não conformidades potenciais, ações preventivas são definidas e implantadas com o objetivo de evitar a ocorrência das mesmas. Após a implantação das ações corretivas, faz-se uma avaliação da eficácia das mesmas, antes de seu encerramento.

Uma vez que a estrutura esteja organizada, testada e melhorada, o próximo passo é realizar a auditoria externa para a certificação na norma. No Brasil, atuam na certificação da norma BS 7799-2 empresas como: DNV, BVQI, BSI, DQS, entre outras[3]. Poucas empresas foram certificadas no Brasil, porém a tendência é que cresça o número de empresas certificadas, devido às novas exigências do mercado quanto à segurança da informação, em especial nas relações que envolvem o mercado exterior e onde a segurança é o diferencial competitivo (instituições financeiras, telecomunicações e área médica).

Conforme apresentado, a implantação de um SGSI é um processo que busca continuamente o aprimoramento do modelo de gestão da segurança da informação. Para tal, o acompanhamento e gerenciamento do fluxo como ciclo PDCA devem ser uma constante na organização, seja através de auditorias periódicas ou de ações de melhorias inseridas na rotina diária de administração da informação.

Recomenda-se a geração de um manual de segurança do projeto SGSI, contendo todos os documentos gerados em cada etapa do processo, ou seja: A política de segurança; a análise de risco; o inventário; a declaração de aplicabilidade com os controles específicos ao escopo selecionado; os temos e as políticas de uso dos sistemas e dos serviços oferecidos; os indicadores de acompanhamento; os incidentes registrados e classificados; além dos 28 procedimentos (PR's) e os Instrumentos Normativos (IO's) recomendados na ISO 17799.

---

[3] Uma lista completa dos orgãos certificadores pode ser obtida em (Certification Portal, 2005)

Algumas ferramentas podem ajudar, no processo de implementação e acompanhamento do ciclo PDCA. Dentre elas: sistema de controle de acesso dos usuários, sistema de inventário de hardware e software, sistema de acompanhamento de não conformidades e o sistema de acompanhamento de indicadores.

Após a implantação do SGSI conforme o modelo proposto, a etapa de acompanhamento e gerenciamento do ciclo deve ser uma constante na organização, através de auditorias periódicas e ações de melhorias. A possibilidade de integrar os controles do SGSI ao Sistema de Gestão Integrado implantado permite a execução de um processo de melhoria contínua, pois o ciclo do PDCA é executado regularmente no cronograma das organizações. Além disso, a experiência obtida nos ciclos de auditoria e de implantação das melhorias, com a remoção das não conformidades encontradas, pode ser utilizada no processo. Neste sentido, a próxima seção apresenta uma breve discussão sobre a integração dos controles do SGSI ao Sistema de Gestão Integrado (SGI), que abrange o Sistema de Gestão da Qualidade – ISO 9001, o Sistema de Gestão Ambiental – ISO 14001 e o Sistema de Gestão de Segurança e Saúde – OHSAS 18001.

4 Correlação entre o Sistema de Gestão da Segurança da Informação e o Sistema de Gestão Integrado

Quando uma organização já possui experiência em implantação de outras normas, o processo de implantação do SGSI ocorre de forma mais fácil, pois é possível aproveitar algumas das ferramentas de gestão e controle já implementados, realizando apenas a adição dos controles relativos à segurança da informação ao SGI existente.

Conforme o Anexo C da **BS 7799-2**, muitas são as interações entre esta norma de segurança e as **ISO 9001** e **14001**. Os procedimentos, instrumentos normativos, padrões e sistemas de gestão já utilizados por empresas certificadas nestas duas últimas normas, podem ser reaproveitados, utilizando as experiências anteriores como base para adicionar novos controles específicos da **BS 7799** (conforme a aplicabilidade destes controles ao escopo da organização). Torna-se possível também incluir estes novos controles nos ciclos de auditorias de acompanhamento dos sistemas de gestão da **ISO 14001** e/ou da **ISO 9001**, acrescentando a este ciclo os controle da **BS 7799**.

Desde de 1987, os princípios advindos das normas série ISO 9000 foram utilizados por diversas empresas para abordar as questões de qualidade, segurança e saúde do trabalhador e questões ambientais, pois permitiam uma estruturação adequada para tratar tais assuntos.

O crescimento do número de empresas que implementaram Sistemas de Gestão de Qualidade, com base nas normas ISO 9001, ISO 9002 e ISO 9003 foi bastante significativo (o número aproximado de certificações até dezembro de 2002 era de 560.000). Por esta razão, as normas ISO 14001 e o guia BS 8800, criados em 1996, e mais recentemente, as normas BSI-OHSAS 18001 e BS7799-2 foram desenvolvidas de modo a permitir a integração (ou seja, a adição) dos requisitos específicos para os seus propósitos, sem com isso apresentar requisitos conflitantes, o que poderia resultar em um entrave para sua disseminação. Como exemplo deste fato, pode-se citar a utilização de um único procedimento para o controle de documentação que trata de forma comum todos os documentos relativos à gestão da qualidade, ambiental, saúde e segurança, além de segurança da informação.

Tabela 1 – Matriz de Correlação de Normas

SGSI		Sistema de Gestão Integrado – SGI					
BS 7799-2:2002		ISO 9001:2001		ISO 14001:1996		OHSAS 18001:1999	
Req.	Especificação	Req.	Especificação	Req.	Especificação	Req.	Especificação
0	Introdução	0	Introdução	0	Introdução		
1	Escopo	1	Escopo	1	Escopo		
2	Normas de Referências	2	Normas de Referências	2	Normas de Referências		
3	Termos e definições	3	Termos e definições	3	Termos e definições		
4	Requisitos para o Sistema de Gerenciamento da Segurança da Informação	4	Requisitos para o Sistema de Gerenciamento da Qualidade	4	Requisitos para o Sistema de Gerenciamento Ambiental		
4.1	Requisitos Gerais	4.1	Requisitos Gerais	4.1	Requisitos Gerais	4.3	Planejamento
				4.3.1	Aspectos Ambientais	4.3.1	Identificação de Perigos, Avaliação de Riscos, Controle de Riscos
4.2	Modelo de Processo	4.2	Modelo de Processo				
4.3	Documentação		Sistema de Gerenciamento da qualidade				
4.3.1	Requisitos gerais	4.2.1	Requisitos gerais	4.1	Requisitos gerais		
4.3.2	Manual do SGSI	4.2.2	Manual da Qualidade	4.4.4	Sistema de Gerenciamento ambiental	4.4	Implementação e Operação
4.3.3	Controle de Documentação	4.2.3	Controle de Documentação	4.4.5	Controle de Documentação		
		7.2.1	Requisitos legais	4.3.2	Requisitos legais	4.3.2	Requisitos legais
4.3.4	Controle de registros	4.2.4	Controle de registros	4.5.3	Registros	4.2.4	Controle de registros
		4.5.3	registros				
5.1	Política de Segurança da Informação	5.1	Comprometimento da direção	4.2	Politica ambiental	4.2	Política de SSO
		5.2	Foco no Cliente				
		5.3	Politica de Qualidade				
		5.5.3	Comunicação Interna	4.4.3	Comunicação	4.4.3	Comunicação
		7.2.3	Comunicação com Cliente				
5.2	Gerenciamento de Recursos	6	Gerenciamento de Recursos	4.4.1	Estrutura e responsabilidades	4.4.1	Estrutura e responsabilidades
		6.2	Recursos Humanos				
		6.3	Infra-estutura				
		6.4	Ambiente de Trabalho				
5.2.1	Provisão de recursos						
5.2.2	Treinamento, consciência e competência	6.2.2	Treinamento, consciência e competência	4.4.2	Treinamento, consciência e competência	4.4.2	Treinamento, consciência e competência
		6.3		4.4.4			
6	Análise crítica do SGSI	5.6	Análise Crítica	4.6	Análise Crítica		
6.2	Auditorias	4.5.4	Auditorias	4.5.4	Auditorias	8.2.2	Auditorias
7	Melhoria Contínua	8.5	Melhoria Contínua	4.3.4	Programa de Gestão Ambiental	4.3.4	Programa de Gestão de SSO
7.1	Melhoria Contínua	5.4.2	Planejamento do sistema de gestão da qualidade				
		8.5.1	Melhoria Contínua	4.2	Politica ambiental		
7.2	Ações corretivas	8.3	Controle deprodutos não conforme	4.5.2	Não conformidades e ações corretivas e preventivas	4.5.2	Não conformidades e ações corretivas e preventivas
		8.5.2	Ações corretivas				
7.3	Ações preventivas	8.5.3	Ações preventivas				

Todas as normas que compõem um SGI possuem o mesmo fluxo para a sua implantação. Desta forma, propõe-se a implantação do SGSI conforme PDCA sugerido na BS7799-2. Buscando utilizar a experiência em implantação de outras normas, a Tabela 1 propõe uma matriz de correlações que permite a adição dos controles do Sistema de Gestão da Segurança da Informação a um Sistema de Gestão Integrado. Esta matriz apresenta as normas que compõem o SGI e as relações destas normas com a norma de Segurança passível de certificação, a BS 7799-2.

A integração entre as normas ilustrada na Tabela 1 facilita a implantação dos controles e o aproveitamento das estruturas de gestão já existentes, reduzindo o tempo de implantação do SGSI e favorecendo o envolvimento e participação dos colaboradores da organização. Muitos são os benefícios desta abordagem, dentre os quais:

- Ganho significativo na rotina de auditoria, pois a mesma equipe de auditores certificados para as demais normas podem ser capacitados para acrescentar em suas auditorias os controles do SGSI;
- Reuniões únicas do comitê de auditores para realizar as análises crítica;
- Aproveitamento de procedimentos e instruções operacionais já existentes, acrescentando os controles do SGSI e escrevendo novos padrões seguindo o modelo já existente;
- Aproveitamentos dos softwares/sistemas de controles já implantados para gestão das não conformidades, gestão dos procedimentos e instruções operacionais, controle de legislação e acompanhamento de indicadores;
- Treinamentos e/ou palestras de conscientização unificadas;
- Geração de um manual único do SGI e;
- Possibilidade de auditorias integradas para acompanhamento ou mesmo re-certificação.

5 Metodologia

A metodologia adotada no trabalho foi baseada nas seguintes etapas:

- Estudo e compreensão do problema e do domínio através do levantamento de referências relacionadas à análise, implantação de um SGSI;
- Definição do escopo do projeto a partir da experiência profissional na implantação e gestão de redes de computadores da autora desta dissertação.
- Proposição, tendo como base diversos documentos, padrões e normas de referência na área de segurança da informação, de uma metodologia de auxílio o planejamento e a implantação de um SGSI em um ambiente computacional em rede.
- Implantação e avaliação da metodologia em um ambiente de produção.

O objeto da pesquisa, a implementação e validação das etapas da metodologia proposta, foi atingido com um estudo de caso envolvendo a empresa Cetrel S/A. A análise dos resultados obtidos é apresentada na próxima seção do trabalho.

6 Conclusão

Logicamente pode-se concluir que o processo de busca de soluções para os problemas de segurança em ambientes computacionais envolve a necessidade do desenvolvimento de padrões, os quais serão tanto utilizados no apoio à construção de sistemas computacionais "seguros", como para a avaliação dos mesmos. A existência de um SGSI implantando na organização, permite ao usuário tomar conhecimento do quão protegidas e seguras estarão as suas informações. Do ponto de vista dos profissionais técnicos, eles passarão a possuir um modelo de atuação comum, evitando assim que cada equipe tenha para si um padrão desconexo das demais equipes. Uma grande contribuição da metodologia é permitir que o responsável pelo projeto tenha uma visão única do sistema de segurança da informação e dos diversos padrões, controles e métodos que o compõem. Isso o habilita

também a verificar a possibilidade de integração dos controles de segurança ao Sistema de Gestão Integrado existente na organização.
As etapas de implantação do SGSI envolveram um nível mais gerencial, e não necessariamente técnico. A implementação e manutenção de um SGSI exigem uma dedicação e análise profunda do ambiente computacional e organizacional. Esta não é uma tarefa fácil e necessita do apoio da direção da organização e a participação dos funcionários. Além disso, o processo poderia envolver a participação de terceiros, como clientes e fornecedores, bem como a contratação de uma consultoria externa. Por tudo isso, tornar seguro um ambiente computacional pode ser uma tarefa bastante complexa, requerendo gestão e procedimentos apropriados.
O projeto de gestão de segurança da informação desenvolvido teve como referência o ambiente computacional da empresa Cetrel S.A, possibilitando validar a metodologia neste ambiente. A oportunidade de utilizar este ambiente de produção para implantar a metodologia explicitou as principais dificuldades encontradas na implantação de um SGSI.
O projeto desenvolvido e implantando, além de utilizar a BS7799/2 como base, resultou no desenvolvimento de uma metodologia própria para a elaboração e implementação de forma clara e objetiva o programa de gestão da segurança da informação, utilizando como suporte a NBR ISO/IEC 17799 e outros importantes padrões de segurança. Ao todo esta ISO contempla 127 controles além daqueles que não foram citados na norma. Porém, para se atingir o patamar de segurança desejado nem sempre é necessária à adoção de todos estes mecanismos, mas sim uma seleção criteriosa dos controles a partir da realização de uma análise de risco. Um dos principais resultados alcançados foi justamente a geração de subsídios para o gerenciamento da implementação de um SGSI. Por isso, ele foi desenvolvido levando-se em consideração as etapas do projeto que foram alcançadas, ao invés de detalhes de como foram alcançadas. Assim, as etapas descritas na seção 4 deste artigo devem ser vistas como modelo gerencial. Isto é, elas são, na verdade, documentos (como relatórios, procedimentos, formulários e planos), ao invés de produtos de natureza muito técnica (como, por exemplo, a instalação de um *firewall*). Este fato demonstra a preocupação em desenvolver o esboço de implementação segundo uma linha mais gerencial do que técnica. Desta forma, a abordagem utilizada segue o que parece ser uma tendência das modernas técnicas de gestão, que focalizam mais os resultados obtidos em detrimento dos processos empregados para obtê-los.
Outro ponto importante foi à constatação de que o ciclo necessário para implantação dos controles de segurança é similar ao ciclo já adotado por outras importantes normas. Isto possibilitou à implantação do SGSI a partir da experiência de implantação do Sistema de Gestão Integrado, tornando mais rápido e fácil a integração do SGSI ao modelo de gestão já existente na organização (SIG CETREL, 2002).

Referências

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 9000:2000, 9001:2000 e 9004:2000**. Coletânea de normas de sistema de gestão da qualidade. Rio de Janeiro, 2001.

_____.**NBR ISO 14001**. Sistema de Gestão Ambiental. Rio de Janeiro. 1996.

_____.**NBR 1333**: Controle de acesso para segurança física de instalações de processamento de dados. Rio de Janeiro, 1990.

_____.**NBR 11515**: Critérios de segurança física relativos ao armazenamento de dados. Rio de Janeiro, 1990.

_____.**NBR ISO/IEC 17799**: Tecnologia da Informação - Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2001.

_____.**NBR 11584**: Critérios de segurança física, relativos a microcomputadores e terminais, em estações de trabalho. Rio de Janeiro, 1991.

BRASIL, Decreto Lei n ° 2.848, de 07 de dezembro de 1940**. Institui o Código Penal. Diário Oficial da República Federativa do Brasil**, Poder Legislativo, Rio de janeiro, 08 de dezembro de 1940.

BRASIL. Lei n° 9.609, de 19 de fevereiro de 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da República Federativa do Brasil**, Poder Legislativo, Brasília, DF, 20 fev. 1998.

BSI-OHSAS-18001 BRITISH STANDARD INSTITUITION. Occupational Health and Safety Management Systems – specification. London 1999.

COBRA. **Consultative, Objective & Bi-functional Risk Analysis, Iso Compliance Analyst,** Release 3.1.8b. C&A Systems Security Ltd. 2002.

DRAFT **BS 7799-2:2002**: Information security management – specification for information security management systems. British Standard Institute, London, 2001.

DRAFT **ISO/IEC TR 19791**: IT security techniques – Security assessment of operational systems. DIN Deutsches Institut für Normung e. V., 2004.

DRAFT **ISO/IEC FCD 18045**: IT Security techniques – Methodology for IT Security Evaluation, DIN Deutsches Institut für Normung e. V., 2004.

DRAFT **ISO/IEC TR 15443-1**: Information technology - Security techniques. DIN Deutsches Institut für Normung e. V., 2004.

DRAFT **ISO/IEC TR 15446**: Information technology - Security techniques – Guide for the production of Protection Profiles and Security Targets. DIN Deutsches Institut für Normung e. V., 2004.

IEC 61508-n, Functional safety of eletrical/electronic/programmable electronic safety-related systems. Commission Electrotechnique Internationale, 1998.

IETF – Internet Engineering Task Force. **Request for Coments (RFC) nº 2828.** GTE/BBN Technologies, 2000. **URL**: http://www.ietf.org/rfc/rfc2828.txt Acessado em: 01 maio 2004.

ISO 9001, Guidelines for the Management of IT Security (GMITS). International Organisation for Standardisation, Switzerland, 1998.

ISO/IEC TR 13335-n, Guidelines for the Management of IT Security (GMITS). International Organization for Standardization, Switzerland, 1998.

ISO/IEC 15408-n, Information Technology – Security Techniques – Evaluation Criteria for IT Security. International Organization for Standardization, Switzerland, 1999.

ISO/IEC 17799 Information Technology - Código de prática para a Gestão da Segurança da Informação. International Organization for Standardization, Switzerland, 2000.

ISO/IEC 19791. International Organization for Standardization, Switzerland, 2004.

ITSEC - Department of Trade and Industry**. The European Information Technology Security Evaluation Criteria**. London, Jun. 1991.

MSF. Microsoft Solutions Framework. **URL**: <http://www.microsoft.com/brasil/security/guidance/prodtech/win2000/secmod134.mspx # XSLTsection121121120120>. Acesso em: 20 Jl. 2004.

MSIA - **Microsoft Software Inventory Analyzer**. Versão 2.1.0.0220. 2004.

NBR ISO/IEC 17799. Tecnologia da Informação - Código de prática para a Gestão da Segurança da Informação. ABNT, Rio de Janeiro, 2001.

NBR 11584. Critérios de segurança física, relativos a microcomputadores e terminais, em estações de trabalho. Julho 1991.

NBR 11515. Critérios de segurança física relativos ao armazenamento de dados. Dez. 1990.

NETWORK. **Network Inventory Master**. LE Software Sweden, Versão 3.0.2004. **URL**: <http://www.abacus.cc/template3.asp?id=41&menu= 0?=eng>. Acesso em: Jan. 2004.

SIG. **Manual do Sistema Integrado de Gestão da CETREL S.A.** 2002.

TCSEC, DEPARTMENT OF DEFENSE. Trusted Computer System Evaluation Criteria, Dec.1985. **URL**: <http://www.radium.ncsc.mil/tpep/library/rainbow/index.html>. Acesso em ago. 2002.

WEBCENSUS, **Tally Systems WebCensus Service**. 2004. **URL**: <http://www.tallysystems.com/products/WebCensus/>. Acesso em Ago. 2003.

XISEC. **XISEC - Empresas certificadas no Brasil**. **URL**: <http://www.xisec.com> Acesso em Ago.2002.