Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação

Alaíde Barbosa Martins (Cetrel S.A. – Empresa de Proteção Ambiental) - alaide@cetrel.com.br
Celso Alberto Saibel Santos (Núcleo de Pesquisa em Redes de Computadores (NUPERC) Universidade Salvador) - saibel@unifacs.br

Este artigo apresenta uma proposta de metodologia para a implantação de um Sistema de Gestão da Segurança da Informação (SGSI). A metodologia é baseada nos principais padrões e normas de segurança, definindo um conjunto de diretrizes a serem observadas para garantir a segurança de um ambiente computacional ligado em rede. O processo de implantação do SGSI 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 e de seus parceiros. Os conceitos e idéias aqui apresentados foram aplicados em um estudo de caso envolvendo a empresa Cetrel S.A. – Empresa de Proteção Ambiental. Para esta empresa, responsável pelo tratamento de resíduos industriais provenientes do Pólo Petroquímico de Camaçari-BA e de outras regiões, a garantia da confidencialidade e integridade dos dados de seus clientes, além da possibilidade de disponibilizar informações com segurança são requisitos fundamentais de funcionamento.

Palavras-chave: segurança da informação, ISO/IEC 17799, gestão de segurança da informação, sistema integrado de gestão

1 Introdução

Apesar da diversidade de trabalhos relacionados ao tema segurança, 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 apresenta uma metodologia teórico-conceitual para auxiliar a concepção, elaboração e implantação de um SGSI em uma organização, a qual está baseada numa série de padrões e normas internacionais (TECSEC, 1985), (ISO 15408:1999), (ISO/IEC TR 13335:1998), (BS7799-2:2001), (ISO/IEC 17799:2001), (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.
O artigo está organizado em 5 seções após esta parte introdutória. A seção 2 apresenta um estudo minucioso dos padrões e normas representativos da área de segurança da informação, os quais devem servir de base para a implantação de um SGSI. A seção 3 apresenta as linhas gerais do processo de implantação de um SGSI. A principal

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

contribuição deste trabalho, uma metodologia para implantação de um SGSI, é apresentada na seção 4. Finalmente, na seção 5 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 Normas e padrões de 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).

2.1 O Padrão BS7799 e a Norma ISO/IEC 17799

O objetivo destas normas é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas empresas. Eles também se destinam a fornecer uma base comum para o desenvolvimento de normas e de práticas efetivas voltadas à segurança organizacional e também, a estabelecer a confiança nos relacionamentos entre as organizações.

A origem da ISO/IEC 17799 data do final da década de 80. Em 1987, no Reino Unido, o *Department of Trade Centre* (DTI) criou o *Comercial Computer Security Centre* (CCSC) com o objetivo de auxiliar as companhias britânicas que comercializavam produtos para segurança de Tecnologia da Informação (TI) através da criação de critérios para avaliação da segurança.

O CCSC surgiu também com objetivo de criar um código de segurança para os usuários das informações, o que resultou, em 1989, na publicação da primeira versão do código de segurança, denominado PD0003 – Código para Gerenciamento da Segurança da Informação. A partir deste ano, vários documentos preliminares foram publicados por esse centro, até o surgimento da BS7799 em 1995. Esse documento foi disponibilizado em duas partes para consulta pública, a primeira em 1995 e a segunda em 1998. Em maio de 2000 o BSI homologou a primeira parte da BS7799. Em outubro do mesmo ano, na reunião do comitê da ISO, a norma foi votada e aprovada pela maioria dos representantes. Em dezembro de 2000, após incorporar diversas sugestões e alterações, a BS7799 ganhou status internacional com sua publicação na forma da ISO/IEC 17799.

A BS7799–1[2] – *Code of Practice for Information Security Management* – é a primeira parte da norma e contém uma introdução, definição de extensão e condições principais de uso da norma. Ela apresenta 10 cláusulas que agrupam controles e objetivos de controles com o intuito de direcionar a gestão e o suporte para segurança da informação.

A BS7799–2 – *Specification for Information Security Management Systems*, publicada em 1998 e revisada em 2002, mas ainda não homologada, é a segunda parte da norma que define as bases necessárias para um SGSI.

Um SGSI é um sistema de gestão análogo a um Sistema da Qualidade e como tal é passível de certificação. Esta certificação se dá a partir das evidências (documentos e práticas) do conjunto de controles implantados e que devem ser continuamente

[2] Nas siglas envolvendo padrões e normas, o último dígito refere-se a uma parte específica da norma ou padrão em questão. BS7799-1 refere-se à parte 1 do *British Standard* 7799.

executados e devidamente registrados. Este modelo de gestão está baseado no ciclo com melhoria contínua PDCA (*Plan-Do-Check-Act*) mostrado na figura 1.

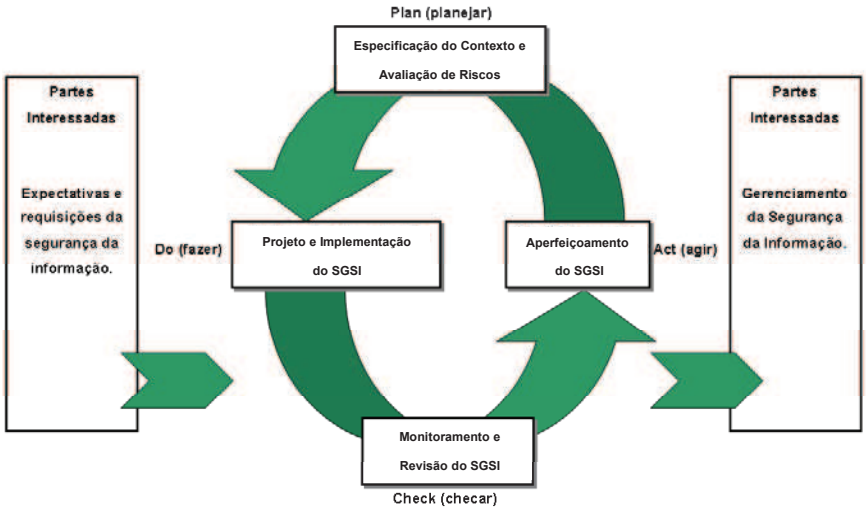

Figura 1 - Ciclo de atividades BS7799-2.

O Ciclo PDCA foi criado em 1920 e ainda hoje, é o principal método da Administração pela Qualidade Total, sendo indicado na BS7799-2 como meio de facilitar o gerenciamento do projeto de Segurança da Informação. O modelo começa com a execução das atividades na fase *Plan*, passando para as fases *Do*, *Check* e *Act*, sucessivamente. A idéia é que este processo seja executado continuamente e que a cada novo ciclo, o sistema seja melhorado.

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. 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. No contexto deste trabalho, outros padrões e normas foram analisados, dentre os quais podem ser destacados ISO/IEC 13335 e IEC 61508.

2.2 A Norma ISO/IEC TR 13335

Formalmente denominada de *Guidelines for the Management of IT Security* (GMITS), a norma (ISO/IEC TR 13335:1998) é composta por 5 partes envolvendo a área de TI:

A Parte 1 – *Concepts and Models for IT Security*, publicada em 1996, fornece uma visão geral dos conceitos e modelos fundamentais usados na gestão de segurança de TI.

A Parte 2 – *Managing and Planning IT Security* – da norma, publicada em 1997, trata do relacionamento da área de segurança da informação com as demais áreas da organização, principalmente a área de segurança corporativa. De maneira semelhante ao padrão BS7799, a Parte 2 sugere a criação de um comitê interdisciplinar que envolva as

diversas áreas da empresa principalmente os responsáveis pelos ativos e pelas informações. Este comitê deve reunir-se periodicamente para definir os níveis aceitáveis de risco, cobrar e acompanhar resultados e reavaliar o projeto de segurança da informação quando necessário. A cláusula 7 da Parte 2 especifica um fluxo de planejamento e gerenciamento do projeto de segurança da informação, além de definir uma série de responsabilidades, com a orientação das atribuições dos atores do processo.

Publicada em 1998, a Parte 3 – *Techniques for the Management of IT Security* – descreve técnicas de gestão de segurança para a área de TI. Ela pode ser utilizada em conjunto com a norma BS7799-2, que sugere quais os processos (e não apenas as técnicas, como na ISO 13335-3) devem ser implantados na condução da gestão de segurança. Vale observar ainda que a Parte 3 trata a gestão de risco em praticamente todas as cláusulas, através de técnicas de análise de risco.

A Parte 4 – *Selection of Safeguards* – foi publicada em 2000 e fornece um catálogo de contramedidas e um guia para a seleção destas.

A Parte 5 – *Management Guidance on Network Security* – complementa a parte 4 da norma, acrescentando fatores relevantes para a conexão de sistemas em redes, tendo sido publicada no ano de 2001.

Outra norma importante para a construção do SGSI, principalmente se o projeto envolver sistemas de automação, é a IEC 61508.

2.3 A Norma IEC 61508

A norma internacional (IEC 61508:1998) enfoca, através de uma abordagem genérica, as atividades do Ciclo de Vida de Segurança para os Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES) que são utilizados para desempenhar funções de segurança. Neste sentido, esta norma vem sendo elaborada com o objetivo de desenvolver um policiamento técnico consistente para todos os sistemas elétricos/eletrônicos relacionados com a segurança.

Os principais objetivos desta norma são: (a) tratar sistematicamente todas atividades do ciclo de vida de um sistema instrumentado de segurança; (b) habilitar que os desenvolvimentos tecnológicos dos produtos se realizem em ambiente sistemático de segurança funcional; (c) ressaltar as melhorias dos *Programmable Eletronic Safety* (PES) nos aspectos de desempenho e de viabilidade econômica e; (d) uniformizar conceitos e servir de base para elaboração de normas setoriais.

Embora esta norma esteja sendo direcionada para sistemas elétricos/eletrônicos de segurança, evidentemente sua orientação pode ser aproveitada em sistemas de segurança implementados através de outras tecnologias, como por exemplo, mecânica, hidráulica ou pneumática. Esta norma está subdividida em 7 partes. As partes 1, 2, 3 e 4 da IEC 61508 são publicações de segurança básicas, tendo, respectivamente, as seguintes denominações: (1) Requisitos Gerais; (2) Requisitos para Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES); (3) Requisitos de Software e; (4) Definições. As partes 5 e 6 apresentam, respectivamente, um Guia para Aplicação da Parte 1 (métodos de determinação dos níveis de integridade de segurança) e um Guia para a Aplicação das Partes 2 e 3. A parte 7 contém uma Bibliografia de Técnicas e Medidas.

A norma IEC 61508 adota uma abordagem baseada em risco, tratando-o como uma combinação de probabilidades e conseqüências de ocorrência. O termo utilizado, Segurança Funcional, é uma característica de sistemas relacionados com a segurança. Nesses sistemas, o conceito Segurança é uma característica do equipamento, incluindo o sistema de controle associado que pode produzir o risco.

Os níveis de integridade de segurança representam medidas internas do sistema adequadas para lidar com o risco. Este conceito direciona a padronização de duas classes de requisitos que devem ser especificados antes do início do processo de desenvolvimento do sistema de segurança. A primeira classe de requisito diz respeito às Funções de Segurança, que devem ser especificadas através do documento denominado "Especificação dos Requisitos Funcionais de Segurança". A segunda classe de requisitos está relacionada com a Integridade de Segurança, devendo ser documentada através do relatório "Especificação dos Requisitos de Integridade de Segurança".

3 O processo de implantação de um SGSI

A análise detalhada dos documentos apresentados nas seções anteriores permitiu a identificação da superposição dos controles extraídos dos diversos padrões e normas, e também, da complementaridade entre vários de seus aspectos.

A implantação da gestão de segurança da informação começa pela definição de quais dos itens especificados em cada padrão devem ser implementados na organização. Em outras palavras, é necessário definir se os itens do padrão estão adequados às características da organização.

O processo de implantação do SGSI proposto utiliza como referência o modelo PDCA descrito na BS7799-2 e a cláusula 7 da ISO 13335-2.

O sucesso do Sistema Integrado de Gestão organizacional, incluindo a gestão de Segurança da Informação, começa com a garantia de 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*[3]. 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 afastará o departamento de segurança das decisões estratégicas, fazendo com que este se torne um departamento meramente operacional da área de Tecnologia da Informação.
A norma BS 7799-2 norma oferece as ferramentas para a implantação e gestão através do modelo PDCA. 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.

---

[3] *Security Officer* é definido como sendo a pessoa responsável pela aplicação ou administração da política de segurança aplicada ao sistema [RFC2828].

4 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 nível de 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 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 2 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.

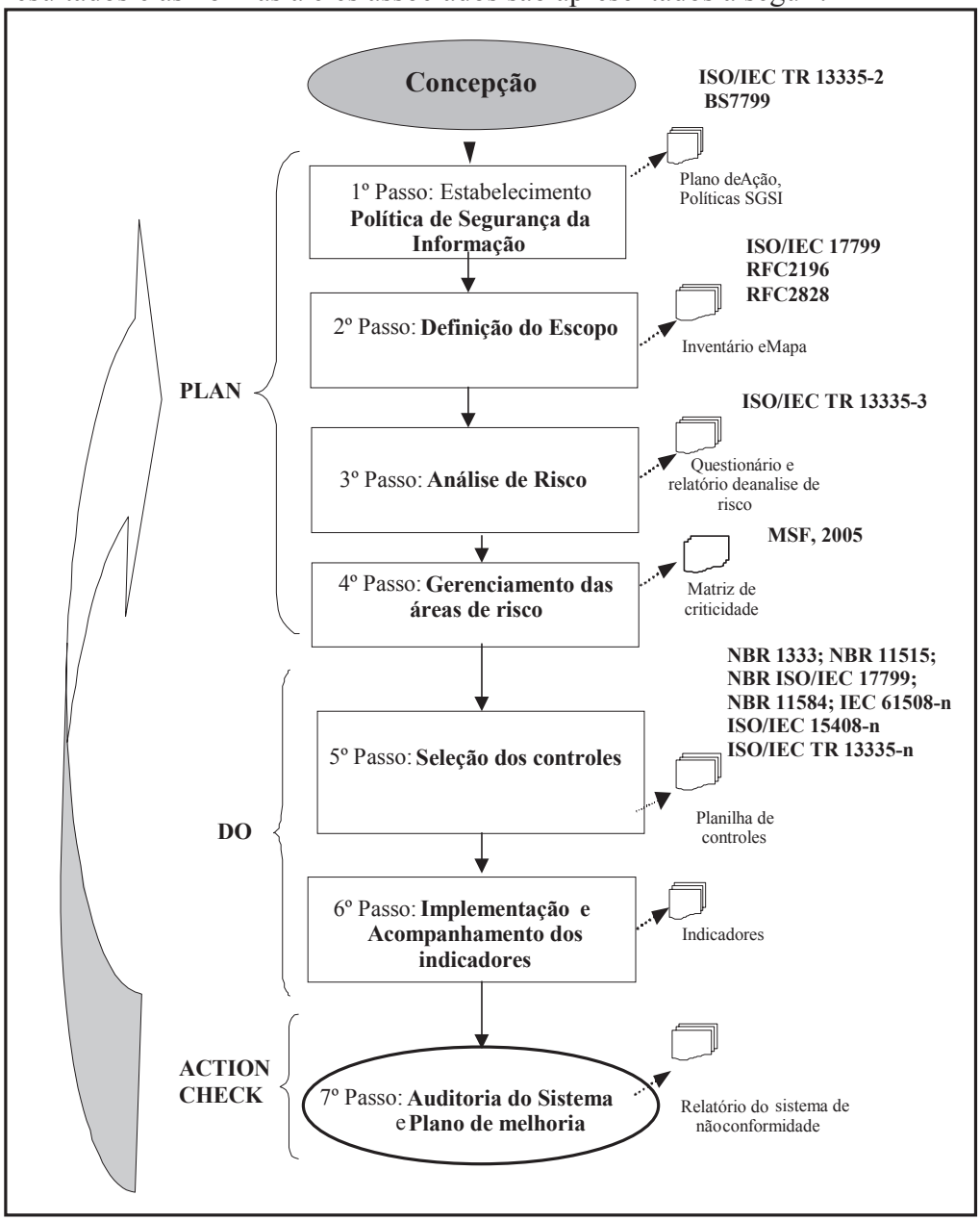

Figura 2 – Proposta de Metodologia para implantação do SGSI.

4.1 A Concepção do Sistema

A etapa inicial, que ocorre antes da realização do primeiro passo da metodologia, corresponde à fase 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. Normalmente, a fase de concepção abrange duas etapas:

1. Diagnóstico da situação atual – verifica-se a existência de alguma política de Segurança da Informação, aproveitando-se de controles já implementados.

2. Planejamento do SGSI e preparação para a sua implantação – nesta etapa, conforme as normas ISO/IEC TR 13335-2 e BS7799, recomenda-se a formação do comitê responsável pela implantação do Sistema na organização. O papel fundamental deste grupo é de realizar formação básica e conscientização dos colaboradores, o planejamento e a preparação do sistema, o detalhamento do projeto e a definição/consolidação da política de Segurança da Informação da empresa conforme as normas e finalmente, o estabelecimento dos objetivos e metas para o Programa de Gerenciamento da Segurança da Informação, em conformidade com o planejamento estratégico da organização.

4.2 Estabelecimento de uma Política de Segurança da Informação

Para construir as políticas de segurança da organização, o comitê deve tomar como base os padrões e normas apresentados anteriormente, sendo que dentre eles, os mais recomendados para esta finalidade são: A BS7799/ISO17799 e as *RFC´s* de número 2196 (1997) e 2828 (2000).

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, sabe-se que não existe uma "Política de Segurança Modelo" que possa ser implementada em toda e qualquer organização, pois a Política deverá ser moldada à especificidade de cada caso. Portanto, elaborar uma Política de Segurança é uma tarefa complexa e que necessita ser constantemente monitorada, revisada e atualizada. Além disso, os seus resultados normalmente só poderão ser notados a médio e longo prazo. É fundamental a existência de uma política de segurança que seja realmente referência para os colaboradores da organização, possibilitando a garantia dos três princípios básicos da segurança da informação: integridade, disponibilidade e confiabilidade.

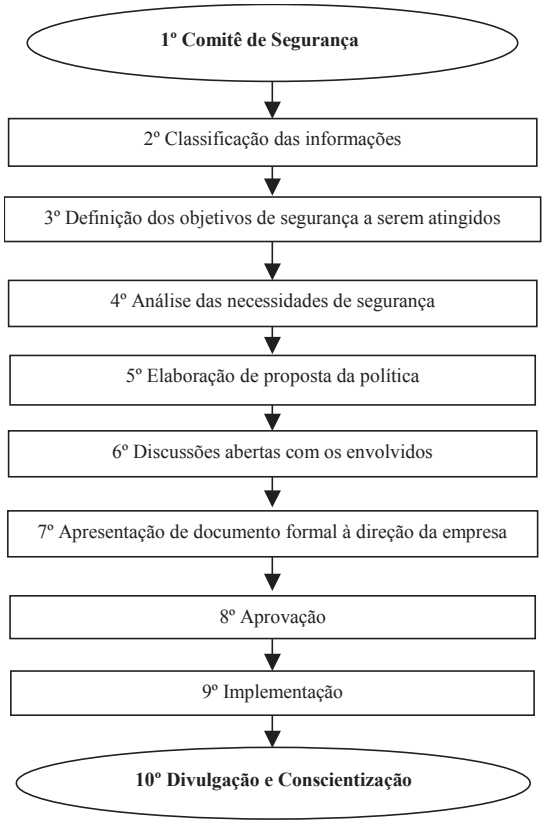

Figura 3 - Fluxograma de desenvolvimento da Política de Segurança da Informação.

O comitê criado deverá ser responsável pela gestão da segurança da informação, portanto, normalmente, este grupo propõe as políticas necessárias para gestão da segurança da informação e seus recursos. Buscando realizar a implantação, acompanhamento e revisões periódicas. Na figura 3, é apresentado o fluxo proposto para o desenvolvimento das políticas de segurança da informação.

A Política de Segurança deverá apresentar algumas características, conforme especifica a ISO/ IEC17799: (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) deve definir as responsabilidades gerais e específicas; (v) deve dispor as conseqüências das violações.

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

- **Propriedade da Informação** – é interessante determinar o responsável pela informação, pessoa que poderá definir quem poderá ter acesso às informações e que nível de acesso é permitido, e qual a periodicidade necessária para a realização do *backup* desta informação.

- **Classificação da informação** – o gestor deverá 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. Deve-se evitar a segregação de função, por exemplo, um mesmo usuário não deve ter acesso à geração de pagamento e liberação do mesmo. É importante, também, que se mantenham as trilhas de auditoria no sistema.

- **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 do usuário proprietário da mesma.

- **Segurança Física** – Os acessos a áreas de servidores 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 deverão ser auditados periodicamente.

- **Desenvolvimento de sistemas ou compra de sistemas/software** – é importante definir uma sistemática interna com ênfase nos requisitos de segurança.

- **Plano de continuidade de Negócios** – é um dos mais importantes tópicos na política de segurança, 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.

4.3 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 interna e externa 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.

Esta etapa produz os seguintes resultados: o mapa do perímetro da rede de computadores onde será aplicado o SGSI; o inventário dos ativos e a classificação desses ativos. A realização do inventário dos ativos da rede (hardware e software) geralmente utiliza ferramentas computacionais específicas, tais como, o software *Network Inventory Master*; a ferramenta gratuita oferecida pela Microsoft MSIA – *Microsoft Software Inventory Analyzer* (MSIA, 2005) voltada ao levantamento de softwares do ambiente Windows; a ferramenta recomendada pela *Business Software Alliance* (BSA), denominada *Tally Systems WebCensus Service*.

4.4 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. Conforme apresentado na seção 3.1, esta norma trata detalhadamente a questão de análise de 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:

a. Reduzir o nível de risco – através da aplicação de controles de segurança.

b. Aceitar o risco – considerar que ele existe, mas não aplicar qualquer controle.

c. Transferir o risco – repassar a responsabilidade de segurança a um terceiro, como, por exemplo, um *data center*.

d. Por fim, negar o risco – esta é a opção menos recomendada.

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 a sua agilidade, geralmente as empresas tendem a adotar o modelo qualitativo, que não requer cálculos complexos. Independentemente do método adotado, uma Análise de Riscos deve contemplar algumas atividades, como o levantamento de ativos a serem analisados, definição de uma lista de ameaças e identificação de vulnerabilidades nos ativos.

O relatório de análise de risco deve conter identificação e classificação de ativos e processos de negócio, análise de ameaças e vulnerabilidades, e análise e parametrização de riscos e definição de tratamento dos riscos.

4.5 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.

Nessa etapa 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.

Nessa etapa ainda 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.

Todo o processo do gerenciamento das áreas de risco de segurança da informação, praticamente desenvolve-se em nove etapas, conforme a figura 4.

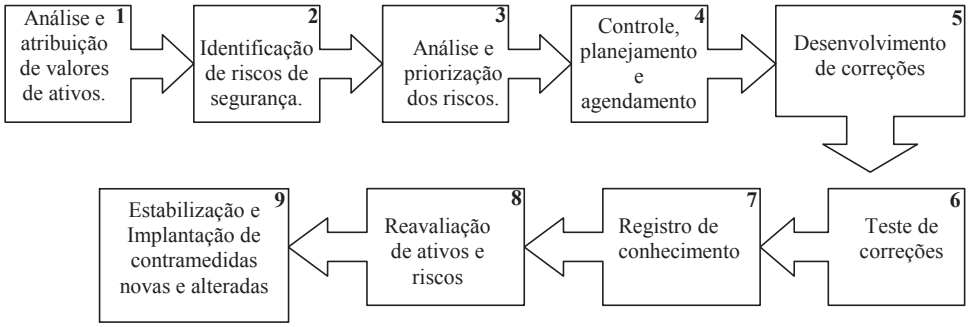

Figura 4 - Gerenciamento das áreas de risco de segurança da informação.

Deve-se buscar implantar a gestão pró-ativa dos riscos, que envolve um conjunto de etapas predefinidas 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. A figura 5 ilustra as quatro etapas da estratégia pró-ativa.

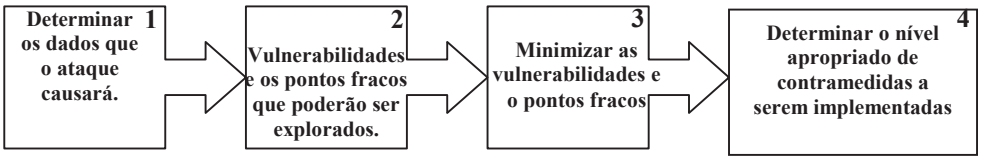

Figura 5 - Etapas da estratégia pró-ativa

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.

4.6 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 na seção anterior).

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 convênios 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, conforme o exemplo da figura 6. Com base nesta declaração, os procedimentos normativos devem ser gerados ou simplesmente revisados de acordo com o sistema normativo já existente na organização.

BS7799-2:2002					
Cláusula	Controle	Objetivo	Aplicável		Referência
3.1		**Política de Segurança**			
3.1.1	**Documento da política de segurança da informação**		**1**		
3.1.2	**Análise crítica e avaliação**		**2**		
4.2		**Segurança Organizacional**			
4.1.1	**Fórum de Segurança da Informação**		**3**		

Figura 6 – Declaração de Aplicabilidade

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.

4.7 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.

4.8 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[4]. 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

[4] Uma lista completa pode ser obtida em (Certification Portal, 2005)

serviços oferecidos; Os indicadores de acompanhamento; Os incidentes registrados e classificados, além dos 28 procedimentos (PR) e os Instrumentos Normativos (IO's) recomendados na ISO 17799.
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 Integrado de Gestão 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.

5 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. A grande contribuição da metodologia é permitir que o responsável pela implementação do projeto de segurança tenha uma visão única do sistema de segurança da informação e dos diversos padrões, controles e métodos que o compõem.
O projeto de gestão de segurança da informação desenvolvido teve como referência o ambiente computacional a empresa Cetrel S.A. 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 obrigaria o apoio da direção da organização e a participação de todos os funcionários com esta finalidade. 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.

A oportunidade de utilizar um ambiente de produção como da empresa Cetrel S.A. para implantar a metodologia desenvolvida, 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 a adoção de todos estes mecanismos, mas sim uma seleção criteriosa dos controles a partir da realização de uma análise de risco.

Uma das contribuições deste trabalho 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 6 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 a 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 Integrado de Gestão, tornando mais rápido e fácil a integração do SGSI ao modelo de gestão já existente na organização (SIG CETREL, 2002).

Referências

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

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

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

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

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

INTERNATIONAL ORGANISATION FOR STANDARDISATION. 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.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508-n, Functional safety of eletrical/electronic/programmable electronic safety-related systems** (1998). Commission Electrotechnique Internationale, 1998.

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

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

INTERNATIONAL ORGANISATION FOR STANDARDISATION. **ISO/IEC 15408-n, Information Technology – Security Techniques – Evaluation Criteria for IT Security** (1999). International Organization for Standardization, Switzerland, 1999.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 17799 Tecnologia da Informação - Código de prática para a Gestão da Segurança da Informação**. International Organization for Standardization, Switzerland, 2000.

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

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 11584, Critérios de segurança física, relativos a microcomputadores e terminais, em estações de trabalho**. Julho 1991.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 11515, Critérios de segurança física relativos ao armazenamento de dados**. Dezembro 1990.

SIG CETREL. (2002) **Manual do Sistema Integrado de Gestão da CETREL S.A.**. Camaçari, Bahia. 2002.

TCSEC, DEPARTMENT OF DEFENSE. (1985) **Trusted Computer System Evaluation Criteria**. December, 1985. Disponível em: <http:// www.radium.ncsc.mil/tpep/library/rainbow/index.html>. Acesso em Ago. 2002.