IMPACTO NA IMPLEMENTAÇÃO DA NORMA NBR ISO/IEC 17799 PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM COLÉGIOS: UM ESTUDO DE CASO

Thiago André Baldissera (UFSM)
thiagoandreb@hotmail.com
Raul Ceretta Nunes (UFSM)
ceretta@inf.ufsm.br

Em um mundo globalizado, competitivo, e com crescentes avanços na área de tecnologia das comunicações e informática, as informações encontram-se presentes em todas as áreas e setores de uma organização. Assim, para as organizações, a informmação passou a ser um dos principais ativos envolvidos no sucesso do negócio, necessitando ser protegida a sua confidencialidade, integridade e disponibilidade. O presente artigo apresenta um estudo sobre a Gestão da Segurança da Informação para as informações digitalizadas de colégios, destacando os aspectos mais relevantes e o impacto para a organização, por ocasião da implementação de controles de segurança baseados na Norma NBR ISO/IEC 17799 na gestão da segurança de informações alicerçadas em recursos de Tecnologia da Informação (TI) de colégios.

Palavras-chaves: Segurança da Informação, Política de Segurança da Informação e NBR ISO/IEC 17799

1. Introdução

Até poucos anos atrás, a questão de segurança da informação em tecnologia da informação em organizações estava intimamente ligada somente à confidencialidade de seus dados guardados em servidores e poucas pessoas tinham acesso a estas informações. Porém, com o grande avanço tecnológico, particularmente nas comunicações e redes de computadores, é cada vez menor a diferença entre coleta, transporte, armazenamento e processamento das informações (TANEMBAUM, 1997).

Hoje encontramo-nos na era da *Sociedade do Conhecimento* (SÊMOLA, 2003), pois a informação é fundamental para qualquer tipo de organização. Por isso, é importante que seja adequadamente protegida, principalmente porque as interconexões no ambiente de trabalho aumentaram significativamente deixando-a exposta a uma grande variedade de ameaças. Como conseqüência, a adequada **Gestão da Segurança da Informação** é uma necessidade inevitável. Gerir segurança significa adotar normas, padrões, diretrizes, dentro outros, que protejam a informação contra os vários tipos de ameaças, minimizando riscos ao negócio e maximizando o retorno sobre os investimentos (ROI).

Conforme Caruso (1999), a maioria das organizações direciona as atenções e investimentos em segurança, apenas nos seus ativos tangíveis físicos e financeiros, mas dedicam pouca atenção e investimentos aos ativos de informação, considerados vitais na sociedade do conhecimento. Logo, para obter a segurança da informação num nível satisfatório, faz-se necessário um conjunto de controles e mecanismos de segurança adequados com intuito de garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

A ABNT (Associação Brasileira de Normas Técnicas), trabalhando em conjunto com a Organização Internacional para Normalização *(International Organization for Standartization – ISO)*, buscou atender as necessidades nacionais no que diz respeito à segurança da informação, disponibilizando a versão brasileira da norma ISO/IEC 17799. A norma da ABNT NBR ISO/IEC 17799:2005 traz as diretrizes e princípios gerais que nos levam a implementar, manter e melhorar a gestão da segurança da informação em uma organização. Entretanto, a norma é ampla e sua adoção pode significar um baixo ROI.

Neste artigo avalia-se o impacto e os pontos mais relevantes da adoção da norma ABNT NBR ISO/IEC 17799:2005, observados a partir da aplicação da norma na gestão de segurança das informações digitais e recursos de informática em colégios.

O artigo está organizado da seguinte maneira: a seção 2 revisa os principais conceitos de gestão da segurança da informação; a seção 3 apresenta uma visão ampla das normas; a seção 4 descreve as etapas de implementação realizadas e a seção 5 discute os aspectos mais relevantes; as conclusões são apresentadas na seção 6.

2. Gestão da Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização. Neste sentido, necessita de proteção adequada contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003). De acordo com a norma NBR ISO/IEC 17799:2005 garantir segurança da informação significa proteger a informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio. Em outras palavras, pode-se dizer que três são os princípios da segurança da informação:

- **confidencialidade:** visa manter informações sigilosas longe de pessoas não autorizadas para terem acesso a elas. Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo;
- **integridade:** visa proteger a informação de modificações não autorizadas, imprevistas ou não intencionais. Assim, toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário; e
- **disponibilidade:** toda informação gerada ou adquirida deve estar disponível aos seus usuários no momento em que eles necessitem dela.

A preservação destes três três princípios constitui o paradigma básico da segurança da informação, mas é importante conhecer seus agentes: ameaças, vulnerabilidades, perímetro, riscos, mecanismos de segurança e responsável pela segurança (*security officer*).

2.1 Ameaças e Vulnerabilidades

O RFC 2828 (2002) define *ameaça* como sendo um potencial para violação dos controles de segurança, o qual existe quando se tem uma circunstância, capacidade, ação ou evento que pode romper a segurança e causar impactos nos negócios. Assim, quanto maior as *vulnerabilidades*, pontos inseguros não gerenciados, maiores são as chances de uma ameaça obter sucesso em seu "ataque", ou seja, maior é o risco ao ativo ou informação.

2.2 Perímetro

Geralmente o alvo de qualquer ameaça é a informação, pois a informação é vital para a organização e hoje seu fluxo está distribuído e compartilhado, ao invés de centralizado. Logo, para planejar segurança significa avaliar o perímetro da informação e reduzir as vulnerabilidades. Conforme exemplo citado por Sêmola (2003), pense em uma casa. O padrão da maioria das casas é de possuir duas portas, uma de entrada ou social e uma de serviço. A finalidade das delas é a mesma, servir como dispositivo de controle de acesso físico. Entretanto, se a porta social três travas e a de serviço uma, elas oferecem **níveis de segurança diferentes**, e houve um desperdício de investimento na porta social, pois dado o perímetro o nível de segurança de uma organização está diretamente associado à segurança oferecida pela 'porta' mais fraca (vide figura 1).

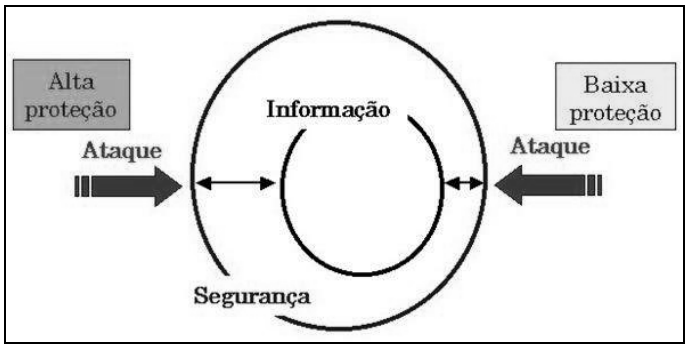

Figura 1 – Segurança = Segurança da "porta" mais fraca

Assim, deve-se analisar se não está havendo proteção demais em certos pontos ou setores e de menos em outros. O conhecimento do perímetro pode minimizar os riscos.

2.3 Riscos

As organizações, independentemente do seu segmento ou do seu tipo, possuem milhares de variáveis que podem se relacionar de maneira direta ou indireta com os seus níveis de risco. Risco é a probabilidade de que ameaças explorem as vulnerabilidades e, desta forma, exponham os ativos, causando impactos maiores ou menores. Tais impactos são limitados por medidas de segurança que protegem os ativos, diminuindo assim o risco.

Considerando ***R*** como sendo a taxa de risco, ***V*** as vulnerabilidades, ***A*** as ameaças, ***I*** os impactos e ***M*** as medidas de segurança; o risco pode ser calculado conforme a equação:

$$R = \frac{V \times A \times I}{M}$$

Observe que a inclusão de medidas de segurança significativa reduz o risco. Por isto a **Análise de Riscos e Vulnerabilidades** é uma das etapas mais importantes para a construção de um sistema de gestão de segurança de informação. Tão importante que o capítulo 4 da NBR ISO/IEC 17799:2005 trata especificamente sobre análise/avaliação e tratamento de riscos. Segundo a NBR, as análises/avaliações de risco devem identificar e priorizar os riscos tendo como base critérios de aceitação dos riscos e dos objetivos da organização.

A tendência atual é a análise de riscos baseada na comparação da existência ou não de controles de segurança, e não mais com o foco principal somente nas vulnerabilidades, por causa da ampla aceitação e credibilidade da norma ISO/IEC 17799 no campo da gestão da segurança da informação. Assim, os responsáveis por segurança não precisam trabalhar nas vulnerabilidades individualmente, mas sim nos controles propostos pela norma, o que também qualifica a organização para uma futura certificação.

2.4 Mecanismos de Segurança

Os mecanismos de controle de segurança são adquiridos, configurados e implementados com a finalidade de atingir o nível de risco aceito em levantamento anterior. Geralmente a atividade de implementação dos mecanismos é realizada pela orientação obtida da Análise de Riscos ou orientada por normas específicas de segurança como a NBR ISO/IEC 17799:2005.

Além dos mecanismos de controle tecnológico, um mecanismo de segurança humano vem ganhando espaço e sendo cada vez mais valorizado pelas organizações: é o profissional de segurança ou o *Security Officer*. O RFC 2828 (2002) define-o como sendo a pessoa responsável pela aplicação ou administração da política de segurança aplicada a todo o sistema.

O *Security Officer*, em virtude das grandes atribuições e responsabilidades, preferencialmente deve estar no mesmo nível dos executivos da organização. Algumas habilidades são fundamentais para este profissional, tais como: possuir perfil tecnológico, saber conduzir projetos, facilidade de comunicação, habilidade de mobilizar pessoas, e seriedade e credibilidade.

3. Normas de Segurança da Informação e Norma NBR ISO/IEC 17799:2005

As normas foram criadas para estabelecerem diretrizes e princípios para melhorar a gestão de segurança nas empresas e organizações (HOLANDA, 2006). Na área de segurança da informação, duas normas auxiliam o *security officer* (ROCHA, 2006): as normas BS *(British Standard)* 7799 e ISO/IEC 17799. No ano de 2000 a ABNT resolveu aceitar a norma ISO como padrão brasileiro, surgindo em 2001 a **NBR 17799:2001** – Código de Prática para a Gestão da Segurança da Informação.

Porém, em 2005 surgiu a norma ISO 27001, que é a BS7799-2:2002 revisada, com melhorias e adaptações contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão já incorporaram (CAUBIT, 2006). No mesmo ano foi também aprovada e publicada pela ISO a norma ISO 27002. No Brasil, a ABNT publicou a sua equivalente como norma brasileira **NBR ISO IEC 17799:2005**.

A ISO/IEC 27001 é a norma usada para **fins de certificação** e substitui a norma Britânica BS 7799-2:2002. A norma brasileira NBR ISO/IEC 17799:2005 é um **guia prático** que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Neste sentido a norma se subdivide em 16 capítulos: Introdução, Objetivo, Termos e Definições, Estrutura da Norma, Análise/avaliação e tratamento de Riscos, Política de Segurança da Informação, Organizando a Segurança da Informação, Gestão de Ativos, 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

Por se apenas um guia, muitas são as discussões sobre os diferentes métodos e modelos de gestão de segurança da informação (BORGES, 2003). As próximas seções procuram salientar os aspectos mais relevantes na implementação de gestão de segurança de informação segundo a norma NBR ISO IEC 17799:2005.

4. Procedimentos Metodológicos

Nesta pesquisa foram avaliados os pontos mais relevantes para gerenciamento da segurança da informação digital em colégios, segundo os controles previstos pela norma de segurança da informação NBR ISO/IEC 17799:2005. Para tal, como estudo de caso, o objetivo é avaliar o impacto da implementação da norma no gerenciamento de segurança dos recursos de TI do Colégio Militar de Santa Maria (CMSM). Esta seção descreve cada passo da implementação da norma no CMSM e indica o tempo requerido em cada etapa.

4.1 Levantamento dos Principais Ativos

Ativo vem a ser qualquer coisa que tenha valor para a organização. São ativos os elementos que compõem o processo de manipulação da informação, a contar a própria informação, os meios em que ela é armazenada, transportada e descartada.

Segundo o Capítulo 7 “Gestão de Ativos” da NBR ISO/IEC 17799:2005, se faz conveniente que todos os ativos devam ser claramente identificados e inventariados. Entretanto, neste estudo de caso os ativos em questão ficaram restritos aos recursos não humanos (recursos de tecnologia de informação).

A identificação dos principais ativos foi obtida reunindo os principais gestores do Colégio em reuniões específicas.

Este levantamento foi realizado pelo Chefe da Seção de Informática, o *security officer* do Colégio, e levou aproximadamente cinco dias de trabalho, no qual ocorreram visitações aos diversos setores e foi necessário disponibilidade de tempo dos gestores para as entrevistas.

4.2 Mapeamento da Relevância

Após a identificação dos principais ativos, é necessário mapear a relevância de cada um deles para serem evitados erros na priorização das atividades (SÊMOLA, 2003). A metodologia

aplicada, utilizou-se de uma faixa de valores de 1 a 5 para indicar o grau de relevância (vide Tabela 1).

Para evitar discrepância na priorização das atividades que compõe a solução a para realização deste trabalho foi necessária uma reunião com os principais gestores dos ativos envolvidos, e discussões a respeito da importância de cada um dos ativos para os processos do negocio.

Esta etapa demandou aproximadamente quatro dias de atividades.

ESCALA		AUXÍLIO PARA INTERPRETAÇÃO
1	**Não Considerável**	• Envolve atingir o objetivo do Processo do Negócio gerenciavelmente, podendo provocar impactos irrelevantes.
2	**Relevante**	• Envolve atingir o objetivo do Processo do Negócio gerenciavelmente, podendo provocar impactos consideráveis.
3	**Importante**	• Envolve atingir o objetivo do Processo do Negócio gerenciavelmente, podendo provocar impactos significativos.
4	**Crítico**	• Envolve a paralisação do Processo do Negócio, podendo provocar impactos muito significativos.
5	**Vital**	• Envolve o comprometimento do Processo do Negócio podendo provocar impactos incalculáveis na recuperação e na continuidade do negócio.

Fonte:Adaptado de Sêmola (2003, pag. 91).

TABELA 1 – Escala para classificação da relevância

4.3 Estudo de Impactos CIDAL e Prioridades GUT

Após o levantamento dos ativos e do mapeamento da relevância, foi realizado um estudo para levantar a sensibilidade de cada um deles para o caso da ocorrência da quebra de segurança, particularmente nos quesitos de ***C**onfidencialidade*, ***I**ntegridade*, ***D**isponibilidade*, ***A**utenticidade* e ***L**egalidade (CIDAL)*.

O estudo foi realizado através de entrevista isolada com o gestor do processo, e o mesmo critério de escala de classificação utilizado no mapeamento da relevância foi utilizado aqui, mas sem analisar o todo.

Ainda na entrevista com o principal gestor foi construída a **Matriz GUT:** ***G**ravidade*, ***U**rgência* e ***T**endência (GUT)*.

No que diz respeito à dimensão gravidade, foi feita a análise de quanto grave seria para o processo do negócio a ocorrência de uma quebra de segurança. Na dimensão urgência, o raciocínio foi que em havendo a quebra de segurança, quanto urgente teria que ser a solução das conseqüências do ocorrido. Para tendência, a análise foi feita fundamentada em qual seria a tendência dos riscos de segurança se nenhuma solução preventiva ou corretiva fosse tomada.

A metodologia para a matriz GUT aplica valores de 1 a 5 para indicar o grau de prioridade. Conforme Sêmola (2003), os valores de classificação são multiplicados gerando o chamado GUT Final. Dessa forma a faixa de valores possíveis é de 1 a 125.

Para realização desta etapa foram necessárias reuniões com os principais gestores dos ativos e com o segundo especialista em TI do colégio, o que demandou aproximadamente sete dias.

4.4 Matriz de Análise de Riscos

As técnicas de análise de risco podem ser aplicadas em toda organização, ou apenas em uma parte da mesma. Neste trabalho, uma das principais etapas para a implantação de uma Gestão de Segurança da Informação no Colégio foi a construção da Matriz de Análise de Riscos, conforme recomenda a NBR ISO/IEC 17799:2005.

A matriz possui seis colunas: a coluna que elenca os Ativos, a coluna das ameaças potenciais, a coluna que lista as vulnerabilidades dos ativos, a coluna que mostra a probabilidade da ocorrência da ameaça, a coluna que mensura o impacto do caso da ocorrência do incidente de segurança, e a coluna que aponta as medidas de segurança adotadas para proteger os ativos.

A Tabela 2 mostra a escala de valores utilizados para mensurar a probabilidade da ocorrência da ameaça, e os valores para o impacto caso a ameaça obtenha sucesso.

PROBABILIDADE		IMPACTO	
0	Completamente improvável de ocorrer	**0**	Impacto irrelevante
1	Ameaça ocorre menos de uma vez por ano	**1**	Efeito pouco significativo
2	Ameaça ocorre pelo menos uma vez por ano	**2**	Sistemas não disponíveis por um determinado período de tempo
3	Ameaça ocorrer pelo menos uma vez por mês	**3**	Perda de credibilidade
4	Ameaça ocorrer pelo menos uma vez por semana	**4**	Efeitos desastrosos, porém sem comprometer a imagem da organização
5	Ameaça ocorre diariamente	**5**	Efeitos desastrosos, comprometendo a imagem da organização

TABELA 2 – Escala para classificação da probabilidade e do impacto

Fundamentalmente, existem duas metodologias para orientar a analise de riscos: a quantitativa, voltada para mensurar os impactos financeiros em virtude de uma quebra de segurança; e a qualitativa, orientada por medidas para estimar os impactos provocados pela exploração de uma vulnerabilidade por uma ameaça. Neste trabalho foi utilizada a metodologia qualitativa.

Aspectos que foram considerados para construção da matriz:

- relevância do processo;
- relação do processo e dos respectivos ativos envolvidos;
- projeção do impacto;
- probabilidade da ameaça explorar a vulnerabilidade;
- qualificação das vulnerabilidades presentes junto aos ativos; e
- qualificação das ameaças.

Observa-se que o estudo contemplou ativos físicos e tecnológicos. Deste modo a identificação de ameaças e vulnerabilidades foi orientada por entrevistas com os gestores, através de observação, inspeções físicas presenciais aos ambientes, e pesquisa a documentações.

Os resultados da matriz de análise de riscos foram alinhados aos controles da norma NBR ISO/IEC 17999:2005, e o nível de conformidade foi avaliado com a referida norma.

Em termos de custos, a construção da matriz de análise de risco foi a etapa que mais demandou tempo e empenho por parte do *security officer* do colégio. Para a construção da matriz foram necessárias três semanas de estudos, pesquisas e anotações.

4.5 Política de Segurança da Informaçao

A Política de Segurança da Informação é um documento de alto nível que representa o topo de uma pirâmide de outros documentos que fornecem informação em graus de detalhamento cada vez maiores sobre os padrões e procedimentos a serem aplicados aos dados e sistemas corporativos.

Segundo a NBR ISO 17799:2005, o objetivo da Política é: "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentos pertinentes". Deste modo, a construção da Política de Segurança da Informação do colégio foi confeccionada após a finalização dos trabalhos, mas obedecendo o que preconiza a NBR ISO/IEC 17799, bem como as outras legislações do Exército Brasileiro e a Lei Nº. 3505 – Política de Segurança da Informação para órgãos do Governo Federal.

A Política de Segurança da Informação foi submetida para apreciação da diretoria, sendo aprovada. Após, a mesma foi comunicada para toda a organização (usuários) de forma relevante, acessível e compreensível.

A maior parte do trabalho para a confecção da Política de Segurança para o colégio, refere-se à adequação da política à gama de legislações, portarias e normas que regem a organização Colégio Militar de Santa Maria. O trabalho demandou de reuniões com a direção do colégio para aprovação da Política e duas palestras direcionada a todos os colaboradores para apresentá-la.

5. Análise da Implementação da Norma

Segundo Mukund (2001), deve-se começar entendendo a importância da Segurança da Informação, recebendo treinamento, estudando as necessidades do negócio, assumindo responsabilidades, estimando o risco. Este foi realmente o ponto de partida para implementação da norma: conhecê-la. Isto pode, dependendo da organização e da conformidade pretendida, requerer uma consultoria. No caso do colégio, não foi usado consultoria, assumindo que esta tarefa deva ser realizada pelo *security officer*.

Além disto, não adiantaria apenas o *security officer* do colégio estar ciente dos controles e mecanismos de segurança recomendados pela norma NBR ISO/IEC 17799:2005. Ele necessita participar de um comitê de segurança, que deve envolver diretamente a direção, e dispor de uma metodologia consciente, capaz de orientar os trabalhos e transformar as atividades em redução nos riscos.

As ferramentas metodológicas utilizadas no trabalho foram:

- planilha de identificação de ativos físicos e tecnológicos (5 dias do *security officer* com pouco envolvimento da equipe);
- mapa de relevância (4 dias com reuniões em equipe);
- estudos dos impactos CIDAL e prioridades GUT (7 dias com reuniões em equipe).

Estas ferramentas ajudaram na:

- construção da Matriz de Análise de Riscos (21 dias do *security officer* com pouco envolvimento da equipe);

– confecção da Política de Segurança (10 dias do *security officer* com pouco envolvimento da equipe).

Observa-se que para implementar a Norma NBR ISO/IEC 17799:2005, vários são os requisitos que a organização deve obedecer, como: comprometimento da equipe, investimentos de dirigentes e colaboradores de toda organização, desenvolvimento de projetos de segurança, mapeamento de ativos, estabelecimento de diretrizes e procedimentos, análise de riscos, análise de impactos, planos de continuidade, políticas de segurança, confecção de documentação e auditorias periódicas. Cada um destes requisitos demanda tempo e cada organização deve estar ciente disto antes de iniciar um processo de implementação da norma.

A matriz de análise de risco tende a ser o ponto mais relevante e oneroso do processo de implantação. Porém, salienta-se que a Gestão da Segurança da Informação necessariamente deve passar por uma mudança de paradigma dos colaboradores, a chamada Cultura da Segurança (DONNER, 2006), podendo esta etapa também influenciar no tempo de implantação da norma.

6. Conclusões

A maioria das organizações direciona as atenções e investimentos em segurança apenas nos seus ativos tangíveis físicos e financeiros, mas dedicam pouca atenção e investimentos aos ativos de informação, considerados vitais na sociedade do conhecimento. Este trabalho discute um estudo de caso da implementação da norma NBR 17799:2005 para gerência de segurança da informação em colégios.

Assumindo apenas os ativos da informação do nível tecnológico e de informática, e um *security officer* especializado, o trabalho observou os tempos gastos para utilizar algumas ferramentas metodológicas essenciais que pudessem levar a uma matriz de análise de risco adequada. Como resultado, observou-se que a etapa mais importante e onerosa do processo, conseqüentemente a mais impactante da implementação da norma, é a construção da matriz de análise de risco.

Referências

BORGES, A. *Segurança com Qualidade Total.* Abr. 2003. CSO – Brasil – Edição 02. Disponível em www.modulo.com.br Acesso em: 12 Abr. 2007.

CARUSO, C. A. *A Segurança em Microinformática e em Redes Locais.* São Paulo. Editora: LTC, 1995 CUSTER, Helen; Windows NT .; São Paulo : Makron Books - 1999.

CAUBIT, R. *O que é a ISO 27001, afinal?* 19 Jan. 2006. Modulo Security Magazine. Disponível em www.modulo.com.br Acesso em: 11 Dez 2006.

DONNER, M. *Empresas certificadas em Segurança. O verdadeiro valor.* 24 Mar 2006. Modulo Security Magazine. Disponível em www.modulo.com.br Acesso em: 11 Dez 2006.

HOLANDA, R. *O estado da arte em sistemas de gestão da segurança da Informação: Norma ISO/IEC 27001:2005. 19* Jan. 2006. Modulo Security Magazine. Disponível em http://ww.modulo.com.br Acesso em: 30 Dez 2006.

MUKUND, J. *BS 7799 (ISO 17799) Information Security Management System.* 2001. ISO 17799 and Computer Security News. Disponível em http://www.computersecuritynow.com/papers.htm Acesso em: 20 Abr. 2007.

NBR/ISO/IEC 17799. *Tecnologia da Informação: Código de prática para a gestão da segurança da informação.* ABNT, 2005;

_____. *Tecnologia da Informação: Código de prática para a gestão da segurança da informação.* ABNT, 2001;

RFC 2828 *Request for Comments: internet security glossary*. Disponível em http://www.faqs.org/rfcs/rfc2828.html acessada em 15/11/2006.

ROCHA, L. F. *Ferramentas para uma boa gestão da Segurança da Informação*. 28 Fev. 2005. Modulo Security Magazine. Disponível em www.modulo.com.br Acesso em: 30 Dez 2006.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma visão executiva*. Editora Campus, 2003;

TANEMBAUM, A. S. *Redes de Computadores*. Editora Campus, 1997.