UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM COLÉGIOS: UMA ANÁLISE DA UTILIZAÇÃO DA NORMA NBR ISO/IEC 17799

DISSERTAÇÃO DE MESTRADO

Thiago André Baldissera

Santa Maria, RS, Brasil

2007

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM COLÉGIOS: UMA ANÁLISE DA UTILIZAÇÃO DA NORMA NBR ISO/IEC 17799

por

Thiago André Baldissera

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de Concentração em Tecnologia da Informação, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de
Mestre em Engenharia de Produção.

Orientador: Prof. Raul Ceretta Nunes

Santa Maria, RS, Brasil

2007

Endereço: Rua Erly de Almeida Lima n. 133 – ap. 202, Bairro Camobi, Santa Maria, RS, 97105-120
Fone (55) 3217-0467; Cel (55) 8115-5711; End. Eletr: thiagoandreb@hotmail.com

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Engenharia de Produção

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM COLÉGIOS: UMA ANÁLISE DA UTILIZAÇÃO DA NORMA NBR ISO/IEC 17799

elaborada por
Thiago André Baldissera

como requisito parcial para obtenção do grau de
Mestre em Engenharia de Produção

COMISÃO EXAMINADORA:

Raul Ceretta Nunes, Dr. (UFSM)
(Presidente/Orientador)

Leoni Pentiado Godoy, Dra. (UFSM)

Luciano Paschoal Gaspary, **Dr.** (UFRGS)

Santa Maria, 19 de julho de 2007.

Este trabalho é dedicado a minha esposa Michele, por todo amor, apoio e incentivo constantes.

AGRADECIMENTOS

A Deus, por me dar a vida, e proporcionar a oportunidade de desenvolver este trabalho em instituições de tão distinto valor como a Universidade Federal de Santa Maria e o Colégio Militar de Santa Maria.

Ao professor Raul Ceretta Nunes, uma pessoa de estimado caráter, educação e conhecimento, pela disposição, paciência e empenho dedicados neste trabalho.

À Universidade Federal de Santa Maria pela oportunidade concedida.

A todos os professores do PPGEP, colegas e amigos que contribuíram para a realização deste trabalho.

Aos colegas do Colégio Militar de Santa Maria, por suas colaborações espontâneas para esta dissertação.

Aos meus pais, Milton e Leni, por seus valores pessoais e pelos exemplos que me ajudaram a ser muito do que hoje sou.

À minha linda família. Michele meu grande amor, e Pedro, meu filho adorado que veio trazer luz e alegria para minha vida.

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM COLÉGIOS: UMA ANÁLISE DA UTILIZAÇÃO DA NORMA NBR ISO/IEC 17799

AUTOR: THIAGO ANDRÉ BALDISSERA
ORIENTADOR: RAUL CERETTA NUNES
Data e Local da Defesa: Santa Maria, 19 de julho de 2007.

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 informação passou a ser um dos principais ativos envolvidos no sucesso do negócio, necessitando ser protegida a sua confidencialidade, integridade e disponibilidade. A presente dissertação apresenta um estudo sobre a Gestão da Segurança da Informação em colégios, destacando os aspectos mais relevantes por ocasião da implementação de controles de segurança baseados na Norma NBR ISO/IEC 17799 (Tecnologia da informação – Código de prática para a gestão da segurança da informação) na gestão da segurança de informações alicerçadas em recursos de Tecnologia da Informação (TI). Como resultado esta dissertação apresenta: *(i)* um estudo da Norma NBR ISO/IEC 17799; *(ii)* uma metodologia conhecida para implementação da mesma, e que envolve etapas como a confecção de uma Política de Segurança e a construção de uma Matriz de Análise de Riscos; *(iii)* o tempo e os custos para o cumprimento de cada etapa da metodologia proposta; *(iv)* quais foram os custos no tocante aos recursos humanos envolvidos; e *(v)* quais foram os pontos críticos para o sucesso do trabalho.

Palavras-chave: NBR ISO/IEC 17799, Segurança da Informação, Gestão de Recursos de TI.

ABSTRACT

Mastership Dissertation
Post-graduation in Engineering Production
Federal University of Santa Maria

INFORMATION SECURITY MANAGEMENT IN SCHOOLS: AN ANALYSIS OF THE USE OF THE NORM NBR ISO/IEC 17799

AUTHOR: THIAGO ANDRÉ BALDISSERA
SUPERVISOR: RAUL CERETTA NUNES
Date and Local: Santa Maria, Jul 19th 2007.

In a globalized world, competitive, and with increasing advances in the area of technology of communications and computer science, the information is presented in all the areas and sectors of an organization. Thus, to the organizations, the information started to be one of the main involved assets in the success of business, needing to be protected its trustworthy, integrity and availability. The present dissertation presents a study on the Information Security Management in schools, detaching the most important aspects for occasion of the implementation of security controls based on Norm NBR ISO/IEC 17799 (Information technology – Code of pratice for information for information security management) in the security management of information connected in resources of Information Technology (IT). As result this dissertation presents: *(i)* a study about the Norm NBR ISO/IEC 17799; *(ii)* a known methodology for implementation of the same one and that it involves stages as the confection of Politics of Security and the construction of a Matrix of Analysis of Risks; *(iii)* the time and the costs for the fulfilment of each stage of the methodology proposal; *(iv)* which had been the costs involved in the human resources, and *(v)* which had been the critical points for the success of the work.

Key words: NBR ISO/ IEC 17799, Security of information, Management of Resources from TI.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

BDTD – Biblioteca Digital de Teses e Dissertações

BI – Boletim Interno

BS – *British Standard*

CAPES – Coordenação e Aperfeiçoamento de Pessoal de Nível Superior

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CIDAL – Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade

CMSM – Colégio Militar de Santa Maria

DEP – Departamento de Ensino e Pesquisa

DCT – Departamento de Ciência e Tecnologia

DMZ – *DeMilitarized Zone*

FTP – *File Transfer Protocol*

GUT – Gravidade, Urgência e Tendência

IDS – *Intrusion Detection System*

IEC – *International Engineering Consortium*

ISMS – *Information Security Management System*

ISO – *International Organization for Standartization*

PC – *Personal Computer*

PDCA – *Plan, Do, Check and Action*

PPGEP – Programa de Pós-graduação em Engenharia de Produção

PUC-Rio – Pontifícia Universidade Católica do Rio de Janeiro

RFC – *Request for Comments*

ROI – *Return on Investments*

SERPRO – Serviço Federal de Processamento de Dados

SGE – Sistema de Gestão Escolar

SGSI - Sistema de Gestão de Segurança da Informação

TI – Tecnologia da Informação

UFSM – Universidade Federal de Santa Maria

VPN – *Virtual Private Network*

SUMÁRIO

INTRODUÇÃO

Até poucos anos atrás, a questão da Segurança da Informação em Tecnologia da Informação (TI) em organizações estava intimamente ligada à confidencialidade de seus dados armazenados em computadores tipo servidores e poucas pessoas tinham acesso a estas informações. Atualmente, com a popularização dos computadores pessoais, surgimento dos *notebooks*, das redes locais, da Internet, compartilhamento de recursos e outras tecnologias, fizeram com que a preocupação e os investimentos com a Segurança da Informação crescessem.

Tanenbaum (1997) bem diz, que 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. As organizações, mesmo aquelas que possuem centenas de escritórios e setores dispersos geograficamente podem, através de uma simples tela de computador, analisar e acessar o status e os dados de sua filial mais remota, tudo isso devido a esse avanço na área da informática e comunicações.

Décadas atrás, as informações eram tratadas de forma centralizada e muito pouco automatizadas. Com o avanço da tecnologia em informática e telecomunicações, compartilhar informações passou a ser uma prática comum de gestão e necessária para organizações que procuram agilidade em suas atividades.

Os cenários e ambientes sociais, tecnológicos, educacionais e econômicos têm sofrido grandes mudanças. Os ambientes são muito dinâmicos, nada mais é estático. As tecnologias de informação e comunicação vêm tomando espaço cada vez maior na sociedade, alterando de forma significativa os meios de produção e disseminação do conhecimento (HUGHES, 1997).

Hoje encontramo-nos na era da *"Sociedade do Conhecimento",* (SÊMOLA, 2003), pois a informação é fundamental para qualquer tipo de organização. A informação é um ativo de grande importância. Com o avanço das tecnologias para redes de computadores, as interconexões no ambiente de trabalho aumentaram muito, deixando a informação exposta a uma grande variedade de ameaças. Por isso, é importante que seja adequadamente protegida. Como conseqüência, a adequada **Gestão da Segurança da Informação** é uma necessidade inevitável.

Gerir segurança significa adotar normas, padrões, diretrizes, dentre outros, que protejam a informação contra 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 aos 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 NBR ISO/IEC 17799:2005.

Esta norma é uma síntese de recomendações para as melhores práticas de segurança, e que podem ser aplicadas em qualquer organização. As recomendações da norma são neutras com relação ao tipo de tecnologia a ser aplicada, pois não existe um padrão que funcione em diferentes ambientes de TI, por isso, da flexibilidade que a norma oferece.

1.1 Tema da Pesquisa

Hoje os ambientes são heterogêneos, as empresas possuem equipamentos de informática muito híbridos. Os riscos são diferentes nas diversas arquiteturas de computadores, de redes e ainda por cima com sistemas operacionais diferentes dentro do mesmo local. Existem novas ameaças, e as vulnerabilidades estão sempre aumentando. Dependemos não somente do computador local mas da informação armazenada em lugares diferentes.

A criação da norma NBR ISO/IEC 17799:2005, justifica-se na medida em que as organizações estão mudando seu comportamento quanto a questão da segurança da informação, devido ao aumento dos diferentes tipos de ataque aos seus recursos de TI, outros ativos e informações. As normas ISO e ABNT são resultado de um esforço internacional que consumiu anos de pesquisa e desenvolvimento para se obter um modelo de segurança eficiente e universal.

Atualmente, os profissionais que trabalham na área de segurança da informação encontram uma variedade de materiais didáticos e comerciais sobre ferramentas e metodologias para utilização da norma NBR ISO/IEC 17799:2005 na gestão de segurança da

informação. Porém, muito pouco se tem falado sobre os aspectos relevantes da utilização da norma para segurança da informação, como por exemplo:

- custos para implementação;
- tempo destinado aos trabalhos;
- material necessário; e
- recursos humanos envolvidos.

Na presente dissertação visa-se analisar estes aspectos mais relevantes por ocasião da adoção da norma NBR ISO/IEC 17799:2005 na gestão de segurança das informações digitais e recursos de informática em colégios.

1.2 Justificativa para exploração do tema da pesquisa

Apesar de reconhecer a necessidade de se estabelecer algum grau de segurança nos sistemas, a maioria das organizações deixa este tema para o final da sua lista de prioridades, até a ocorrência de um desastre (NBSO, 2003).

A Gerência costuma ver a segurança em TI por uma perspectiva negativa, como um fator inibidor, responsável pela redução da capacidade operacional da organização (burocratização), em vez de uma atividade que auxilia a organização a alcançar uma melhor qualidade do serviço com menos recursos.

Toda organização deve preocupar-se com a segurança de TI por três razões principais (NBSO, 2003):

1. *Dependência dos sistemas de informação*. Sistemas que ofereçam serviços adequados e no tempo certo são a chave para a sobrevivência da maioria das organizações atuais. Sem seus computadores e sistemas de comunicação, as empresas ficariam incapazes de fornecer serviços, processar faturas, contatar fornecedores e clientes ou efetuar pagamentos. Os sistemas de informação também armazenam dados sigilosos, que, se tornados públicos, causariam embaraço e em alguns casos o fracasso da organização.

2. *Vulnerabilidade dos sistemas de TI*. Sistemas de TI exigem um ambiente estável, pois podem ser danificados por desastres naturais como fogo, inundação ou terremotos, falhas no controle da temperatura ou do suprimento da energia elétrica, bombas, acidentes ou sabotagens. Os sistemas de TI são as chaves para o acesso a

vastas quantidades de dados corporativos, tornando-se um alvo atraente para *hackers*, repórteres, espiões, ou um simples funcionário insatisfeito.

3. *Investimento em sistemas de TI*. Sistemas de informação são caros tanto no desenvolvimento quanto na manutenção, e a administração deve proteger esse investimento como qualquer outro recurso valioso. Bens de TI são particularmente atrativos para ladrões, por serem portáteis e facilmente vendidos.

Assim, a uma correta gestão da segurança da informação em TI justifica-se porque protege a informação contra um grande número de ameaças, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades.

Em colégios essa regra não é diferente. Atualmente os colégios encontram-se informatizados e grande parte das informações importantes para a rotina dos trabalhos gira em torno dos dados geridos por recursos de TI.

Assim, com a realização deste trabalho poderemos responder aos questionamentos das direções e responsáveis pelos recursos de TI de colégios com relação aos pontos que mais se destacam por ocasião da adoção da norma NBR ISO/IEC 17799:2005 para gestão da segurança das informações dependentes dos recursos de TI em colégios.

1.3 Objetivos

1.3.1 Objetivo Geral

Esta dissertação possui como objetivo geral avaliar 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 analisar a implementação da norma no gerenciamento de segurança da informação digital do Colégio Militar de Santa Maria (CMSM).

1.3.2 Objetivos Específicos

- Realizar uma revisão de literatura dos principais tópicos relacionados com Segurança da Informação e a norma NBR ISO/IEC 17799:2005;

- Estudar e compreender a norma NBR ISO/IEC 17799:2005 da ABNT;

- Construir uma Política de Segurança baseada na norma NBR ISO/IEC 17799:2005 para as informações digitalizadas do CMSM;

- Construir a Matriz de Análise de Riscos para os ativos que tenham envolvimento com informações digitalizadas do CMSM; e

- Apresentar índices e dados sobre os principais pontos para uma implementação de Gestão de Segurança de informações digitais tendo como guia a norma NBR ISO/IEC 17799:2005.

1.4 Importância do Trabalho

A principal contribuição da pesquisa é apresentar os pontos mais importantes com relação a aspectos como custos, tempo, recursos humanos e recursos materiais; para a gestão de segurança das informações digitalizadas em colégios.

Pois, como já foi comentado anteriormente, material sobre casos de sucesso da implementação da NBR ISSO/IEC 17799:2005 em organizações e metodologias existem a disposição, porém dados sobre dificuldades e fatores críticos de uma implementação são raros.

Particularmente para o CMSM, o trabalho torna-se importante na medida em que há necessidade de se conhecer as informações digitalizadas mais relevantes do colégio, os principais ativos envolvidos com o processamento e armazenamento destas informações, as principais vulnerabilidades que estes ativos e informações possuem, o impacto que poderá advir no caso de um incidente de segurança em relação a estes ativos e informações importantes. Assim, o trabalho trará contribuições significativas no âmbito administrativo e

tecnológico, pois, implementa uma série de mecanismos para se obter uma melhor gestão da segurança das informações digitalizadas para o colégio em estudo.

1.5 Estrutura do Trabalho

No capítulo 2, têm-se uma visão geral sobre segurança da informação, abrangendo assuntos como: os conceitos básicos para gestão da segurança da informação; normalizações; aspectos a respeito da NBR ISO/IEC 17799:2005, como sua importância, seu surgimento, seu escopo e sua colaboração para certificações; trabalhos e outros estudos relacionados a aplicação da norma NBR ISO/IEC 17799:2005.

No terceiro capítulo, apresenta-se a metodologia proposta para a elaboração de um projeto para gestão de segurança da informação dos principais ativos do CMSM.

No capítulo 4 é apresentada a aplicação da metodologia proposta, descreve-se os resultados obtidos, e apresentam-se a análise da implementação da norma, onde se descreve os pontos mais relevantes, uma discussão sobre o ônus dos trabalhos realizados e custos da implementação.

Finalizando este trabalho, o capítulo 5 discorre sobre as principais conclusões obtidas e as sugestões para trabalhos e pesquisas futuras.

2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Para melhor compreensão do tema deste trabalho, este capítulo discute Segurança da Informação de maneira abrangente, incluindo sua normalização. Adicionalmente, apresenta as principais diretrizes da norma NBR ISO/IEC 17799:2005, bem como faz uma síntese dos trabalhos acadêmicos relacionados à esta norma.

2.1 Segurança da Informação

"**Segurança da informação** é a proteção da 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." (NBR ISO/IEC 17799:2005, p. ix)

"Podemos definir **Segurança da Informação** como uma área do conhecimento dedicado à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." (SÊMOLA, 2003, p. 43)

Nesta seção apresentam-se seus conceitos, mecanismos, políticas e soluções.

2.1.1 Conceitos básicos

A informação é um ativo que, como qualquer outro ativo importante, se faz hoje em dia essencial para os negócios de uma organização, e consequentemente necessita de proteção adequada.

Toda informação possui um ciclo de vida, que por sua vez é composto por todos os momentos em que a informação pode ser colocada em risco. Conforme podemos observar na Figura 01, quatro são os momentos no ciclo de vida da informação merecedores de atenção: *Manuseio*, *Armazenamento*, *Transporte* e *Descarte*. É importante ressaltar que, independente da forma como a informação é mantida, seja papel ou digitalizada, todos os momentos podem ser aplicados.

Segunda a NBR ISO/IEC 17799:2005, três são os princípios da segurança da informação que se tem de preservar (visualizar a Figura 01):

1. **CONFIDENCIALIDADE** – visa manter informações sigilosas longe de pessoas não autorizadas para terem acesso. Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo;

2. **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
3. **DISPONIBILIDADE** – toda informação gerada ou adquirida deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem de forma contínua e ininterrupta.

Outros dois aspectos complementares também são essenciais de serem observados quando das práticas da segurança da informação como:

- **autenticidade:** reconhecimento formal dos elementos que entram em comunicação ou fazem parte de uma negociação; e
- **legalidade:** informações que possuem valor legal dentro de um processo de comunicação.

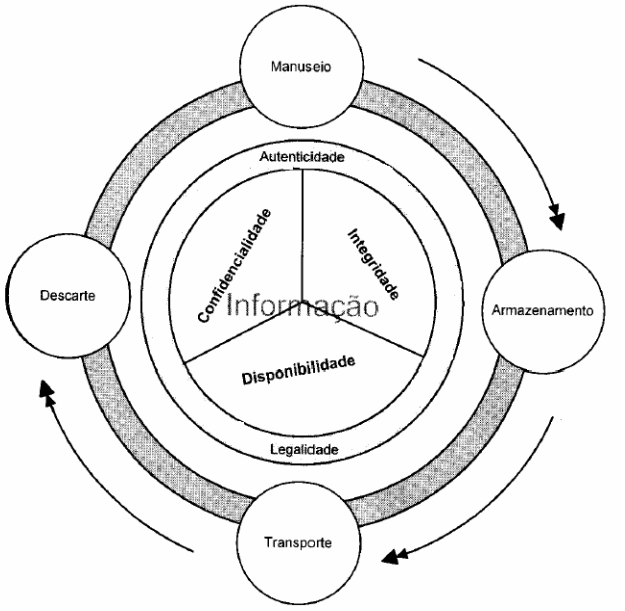


FIGURA 01 – Ciclo de vida da informação considerando os 3 princípios básicos e os aspectos complementares
Fonte: SÊMOLA(2003) pág. 11

O termo "Segurança da Informação" é um termo que pode assumir dupla interpretação: a segurança como **meio** visa garantir a confidencialidade, integridade e disponibilidade da informação, o não repúdio, a conformidade com a legislação vigente e a continuidade dos negócios; e a segurança como **fim** é alcançada por meio de práticas e

políticas para padronização operacional e gerencial dos ativos, e processos que manipulam as informações.

Abaixo se listam outros conceitos de elementos essenciais e participantes da segurança da informação:

⇒ **informação -** é um conjunto de dados utilizados para transferência de uma mensagem entre pessoas ou máquinas em processos. A informação pode estar presente ou ser manipulada por diversos elementos do processo, chamados ativos, os quais são alvos de proteção da segurança da informação;

⇒ **ativo -** termo oriundo da área financeira, pode ser considerado 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;

⇒ **política** - conforme a NBR ISO/IEC 17799:2005, são as intenções e diretrizes globais formalmente expressas pela direção;

⇒ **risco –** a NBR ISO/IEC 17799:2005 define este conceito como sendo a combinação da probabilidade de um evento e de suas conseqüências. Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade;

⇒ **ameaça** - agente ou condição que causa incidentes que comprometem as informações e seus ativos por meio da exploração das vulnerabilidades, podendo provocar perdas de confidencialidade, integridade e disponibilidade, consequentemente causando impactos nos negócios da organização;

⇒ **vulnerabilidade -** fragilidade de um ativo ou de um grupo de ativos que pode ser explorada por uma ou mais ameaças e que permite a ocorrência de um incidente de segurança (NBR ISO/IEC 17799:2005);

⇒ **impacto -** abrangência dos danos causados por um incidente de segurança sobre um ou mais processos e ativos da organização; e

⇒ **incidente -** evento decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, levando à perda de confidencialidade, integridade ou disponibilidade.

2.1.2 Distribuição do investimento em segurança

O alvo de qualquer ameaça geralmente é a informação. Assim, vale ressaltar que hoje em dia a informação não se encontra mais confinada em arquiteturas centralizadas, ou processos únicos. A informação é vital para toda a organização e seu fluxo está distribuído e compartilhado.

A maioria dos executivos e pessoas que fazem parte do nível gerencial das organizações possui a chamada "Visão do Iceberg", pois nos icebergs a porção de gelo que vemos fora da água é aproximadamente 1/5 de todo o gelo. Comparando, muitas vezes nos atemos ao problema da segurança da informação somente a aspectos tecnológicos, ou seja, associamos riscos somente a computadores, vírus, *hackers* e etc.

Existem outros aspectos para os riscos tão relevantes quanto os tecnológicos, como a chamada Engenharia Social onde o foco está na exploração das vulnerabilidades humanas (MACHADO, 2002).

Toda informação pode ser acessada por processos, os quais movimentam o negócio da organização. Em cada processo encontramos vulnerabilidades, e conforme são as vulnerabilidades, medidas de segurança devem ser tomadas. O primeiro anteparo no caso do assédio ou incidência de uma ameaça depende destas medidas. A Figura 02 mostra os perímetros da informação.

A NBR 17799:2005, traz como um dos fatores críticos de sucesso, a necessidade da correta identificação dos elementos internos e externos que interfere nos riscos à segurança, e um bom entendimento dos requisitos de segurança da informação e análise de riscos.

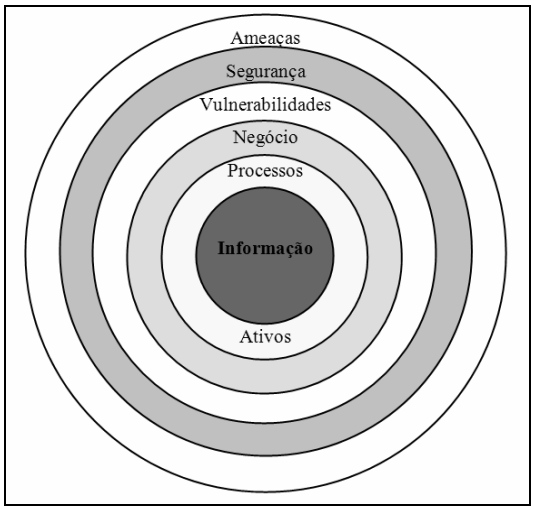


FIGURA 02 – Perímetros

Conforme descrição de um exemplo citado por Sêmola (2003), o padrão da maioria das casas ou apartamentos é possuir duas portas, uma de entrada ou social e uma de serviço. A finalidade das mesmas é a de servir como dispositivos de controle de acesso físico, a pertinência do exemplo está na inconsistência destes dispositivos. A inconsistência encontra-se porque estes dois mecanismos que protegem os ativos (objetos pessoais no interior da residência), não oferecem a mesma resistência, ou seja, não possuem o mesmo tipo de tranca, o mesmo tipo de fechadura, e não são feitas do mesmo material. **A porta social e de serviço oferecem níveis de segurança diferentes**. Assim, o investimento em segurança não foi devidamente distribuído. O nível de segurança de uma empresa ou organização está diretamente associado à segurança oferecida pela 'porta' mais fraca, conforme ilustra a Figura 03.

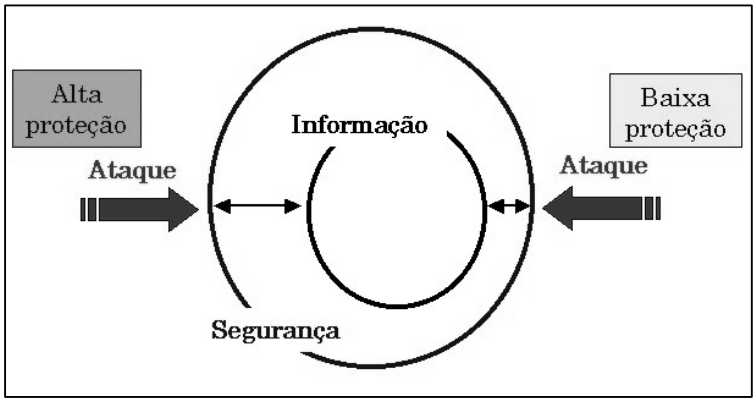


FIGURA 03 – Segurança = segurança da "porta" mais fraca

2.1.3 Principais Ameaças

A *Request for Comments* (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.

Independente das medidas ou mecanismos de segurança implementados, as ameaças podem existir tanto no ambiente externo da organização como no ambiente interno. As ameaças internas por vezes podem ser tão ou mais impactantes do que as ações de ameaças externas, podendo advir de um acesso indevido, de um procedimento incorreto executado por um colaborador, ou até uma ação intencional com a finalidade de causar grandes prejuízos para pessoas ou para a organização, como fraudes, roubos de informações pessoais e sigilosas e etc.

As Figuras 04 e 05 retratam, respectivamente, as principais ameaças e a incidência de ataques e invasões segundo a 9ª Pesquisa Nacional de Segurança da Informação realizada pela empresa Modulo Security em 2003. Observe que os funcionários insatisfeitos encontravam-se em segundo lugar no ranking das principais ameaças a segurança da informação das organizações pesquisadas e entrevistadas, e eram responsáveis por 23% de todos os ataques e invasões identificados.

A Figura 06 demonstra os principais pontos explorados pelos invasores para causar incidentes de segurança nas organizações. Os principais pontos de invasão são a Internet com 60%, Sistemas Internos com 23% e Acesso Remoto com 6%.

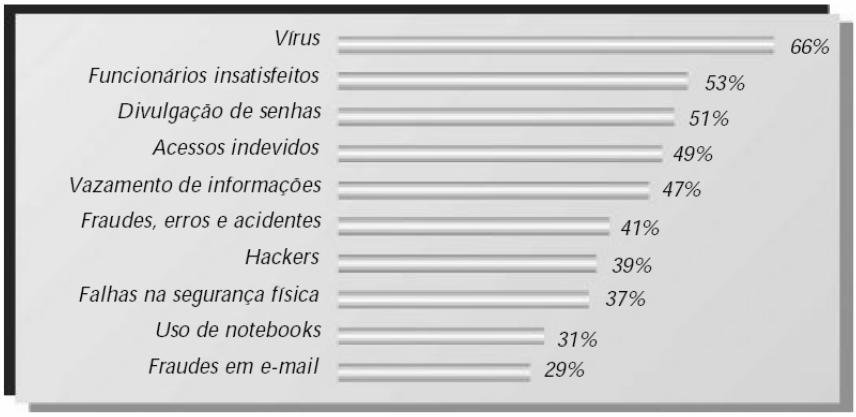


FIGURA 04 – Principais ameaças para a segurança da informação
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003
Obs.: o total é superior a 100% devido as múltiplas respostas

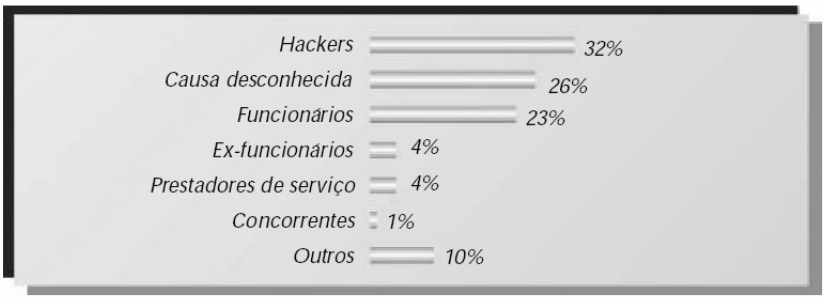


FIGURA 05 – Incidência de ataques e invasões
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003

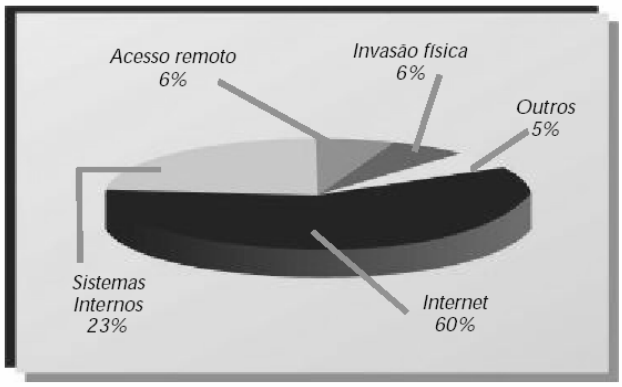


FIGURA 06 – Principais pontos de invasão
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003

A Figura 07 mostra um panorama dos incidentes reportados ao CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), no período de Julho a Setembro de 2006.

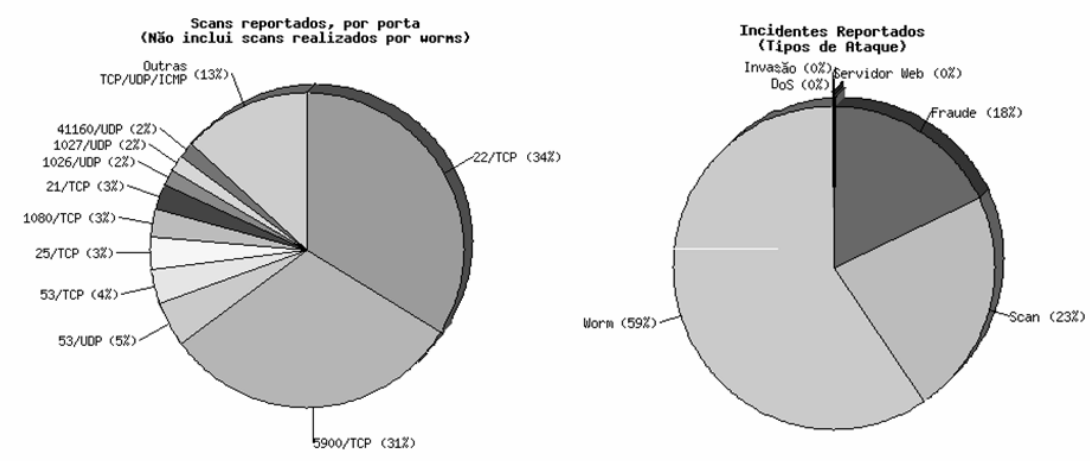


FIGURA 07 – Incidentes reportados ao CERT.BR – Julho a Setembro de 2006
Fonte: CERT.BR (http://www.cert.br)

Conforme a figura acima se pode notar a quantidade de incidentes de segurança no referente aos recursos de rede e servidores. Pois grande parte dos incidentes reportados são *Worms*, Fraudes e *Scans*. *Scans* estes que atacam as diferentes portas dos servidores, sendo as portas 22/TCP (34%) e 5900/TCP (31%) as mais visadas no período considerado.

As ameaças podem assim ser classificadas quanto a sua intencionalidade em:

- **naturais**: decorrentes de fenômenos da natureza, como incêndios naturais, terremotos, tempestades eletromagnéticas, aquecimento, e etc;

- **involuntárias**: ameaças inconscientes, na maioria das vezes causadas pela ignorância e pelo desconhecimento. Podem ser causadas por acidentes, falta de energia, etc; e
- **voluntárias**: ameaças propositais causadas por agentes humanos como *hackers*, invasores, funcionários, disseminadores de vírus de computador, ladrões e etc.

Observe que quando se fala de ameaças não se pode esquecer de comentar sobre vulnerabilidades, porque quanto maior as vulnerabilidades maiores são as chances de uma ameaça obter sucesso em seu "ataque". Portanto, quanto melhor e maior for a "parceria" ameaça/vulnerabilidade maior é o risco ao ativo ou informação.

2.1.4 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.

Conforme Sêmola (2003), risco é a probabilidade de que agentes (ou ameaças) explorem as vulnerabilidades, e desta forma exponham os ativos, causando impactos maiores ou menores. Estes 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 seguinte equação:

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

Segundo a NBR ISO/IEC 17799:2005, não existe segurança 100% ou segurança total. Por isso, se faz necessário às organizações estarem habilitadas a suportar mudanças nas variáveis da equação, e que ações gerenciais adicionais devem ser implantadas para monitorar e melhorar a eficiência e eficácia dos controles de segurança.

Os ativos são alvos de investidas de ameaças de toda a ordem e a todo instante. Conforme se pode constatar na fórmula do risco citada anteriormente, um cenário com alta vulnerabilidade, ameaça e impacto é o que necessita de maiores investimentos. Porém, podem ocorrer variações nas variáveis que são interessantes de se observar. Por exemplo, certo ativo pode ter alta vulnerabilidade porém a probabilidade de ameaça pode ser baixíssima, e o impacto de um incidente sobre este ativo também pode ser baixo, assim os investimentos em medidas de segurança podem ser menores.

A **Análise de Riscos e Vulnerabilidades** é uma das etapas de suma importância para a construção de um sistema de gestão de segurança de informação que funcione. O capítulo 4 da NBR ISO/IEC 17799:2005, trata sobre análise/avaliação e tratamento de riscos.

Segundo a NBR ISO/IEC 17799:2005, as análises/avaliações de risco devem identificar e priorizar os riscos tendo como base critérios de aceitação dos riscos e dos objetivos da organização. Os resultados devem servir como guia para ações de gestão apropriadas e para o gerenciamento dos riscos da segurança da informação, e para implementar a medidas de segurança para proteger os ativos.

As análises/avaliações de riscos devem ser realizadas periodicamente ou sempre que ocorrer mudanças significativas no cenário, pois somente assim será possível contemplar as mudanças nos requisitos de segurança de informação e na situação de risco.

Deve-se compreender que os riscos em que as informações e os ativos de uma organização estão sujeitos não são somente determinados pelas falhas de segurança tecnológica ou das habilidades de quem vão explorá-las, e assim a um conjunto de outras variáveis como aspectos físicos, humanos e legais. A NBR ISO/IEC 17799:2005 afirma que a análise de riscos deve ser aceita como um instrumento de diagnóstico da situação atual da segurança da organização.

Aspectos que devam ser considerados quando de uma análise de riscos:

- relevância do ativo ou informação para o negócio;
- dependência que um ou mais processos do negócio tem do ativo;
- impacto quando da ocorrência de um incidente de segurança;
- probabilidade da ameaça explorar a vulnerabilidade (conjunto ameaça/vulnerabilidade);
- qualificação das vulnerabilidades junto aos ativos; e
- qualificação das ameaças potenciais.

Uma análise deve ser guiada por entrevistas com gestores de ativos, usuários, inspeção presencial das instalações físicas, estudos de documentos e estudo das técnicas dos ativos tecnológicos, para procurar possíveis falhas. O conhecimento das vulnerabilidades, ameaças e medidas de segurança é a base do conhecimento para uma análise de riscos eficiente.

A NBR ISO/IEC 17799:2005 recomenda que a analise/avaliação de riscos possua um enfoque sistemático de estimar a magnitude do risco, e um processo de comparar os riscos estimados contra os critérios de risco para determinação da importância do risco. A construção de uma Matriz de Análise de Riscos é uma das ferramentas utilizadas que podem ser utilizadas na Análise de Riscos e Vulnerabilidades que visa atender esta recomendação da norma. A Tabela 01 apresenta um exemplo de Matriz de Análise de Riscos construída para o ativo "Rede".

TABELA 01 – Exemplo de Matriz de Análise de Riscos

Ativos	Ameaças	Vulnerabilidades	Probabilidade*	Impacto**	Medidas de Segurança
Rede	Utilização de senha por pessoa não autorizada	* Falha na política de criação e alteração periódica de senhas;	2	4	Medidas citados nos planos de segurança que protejam os ativos.
		* Falta de manutenção de senhas dos usuários;	2	1	
		* Falta de atualização no cadastro de usuários da organização (desligamento);	3	1	
		* Utilização de senha padrão do sistema operacional;	5	4	
		* Engenharia social – tentativa de descoberta de informações pessoais do usuário;	1	2	
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

**** Probabilidade:***
0 *- Ameaça completamente improvável de ocorrer*
1 *- Probabilidade de ameaça ocorrer menos de uma vez por ano*
2 *- Probabilidade de ameaça ocorrer pelo menos uma vez por ano*
3 *- Probabilidade de ameaça ocorrer pelo menos uma vez por mês*
4 *- Probabilidade de ameaça ocorrer pelo menos uma vez por semana*
5 *- Probabilidade de ameaça ocorrer diariamente*

***** Impacto:***
0 *- Impacto irrelevante*
1 *- Efeito pouco significativo, sem afetar a maioria dos processos de negócios da instituição*
2 *- Sistemas não disponíveis por um determinado período de tempo, podendo causar perda de credibilidade junto aos clientes e pequenas perdas financeiras*
3 *- Perda de credibilidade*
4 *- Efeitos desastrosos, porém sem comprometer a imagem da instituição*
5 *- Efeitos desastrosos, comprometendo a imagem da instituição*

Com a matriz construída podem-se organizar as prioridades, apoiar as decisões e implementar as medidas de segurança para cada perímetro da organização. É importante

ressaltar que limitações orçamentárias, técnicas, e fatores internos e externos podem impedir a implementação das medidas de segurança especificadas, buscando um nível de risco aceitável para a organização.

A NBR ISO/IEC 17799:2005 recomenda que por ocasião da seleção, implementação e operação de controles de segurança para atender os requisitos identificados na análise/avaliação de riscos, se faz necessário balancear o investimento nestes controles contra a probabilidade de danos por ocasião da falha de segurança. Portanto, também se faz necessário analisar o retorno sobre o investimento no caso de se optar por implementar as medidas de segurança e controle para proteção dos ativos, para diminuir a taxa de risco. Segundo Friedlob (1996), no processo de avaliação de investimentos uma medida financeira comumente utilizada por executivos e administradores é o chamado ROI (*Return on Investments* – Retorno sobre o Investimento), que relaciona investimento e resultado, permitindo apresentar o lucro ou o custo com um investimento

Conforme Lev (2004) o ROI vem sendo muito aplicado no processo de avaliação de investimentos em TI e geralmente é utilizado como justificativa para aprovação de projetos. Dada às características dos projetos de TI, a avaliação do ROI envolve a identificação e a classificação de benefícios tangíveis e intangíveis associados ao investimento. Esses benefícios são posteriormente convertidos em fluxo de caixa permitindo assim a avaliação do investimento e o acompanhamento dos resultados.

O ROI, particularmente para a segurança e a tecnologia, ajuda a reverter o velho paradigma de que muitos acham que aplicar recursos nessa área é despesa e não investimento.

Importante ressaltar, que todo investimento ou aplicação de recursos possui um ponto de inflexão, ou seja, um momento em que o retorno sobre o investimento não é justificável, por exemplo, o custo da implementação de uma medida de segurança é mais cara do que o ativo a que se propõe proteger ou o impacto de um incidente de segurança sobre o mesmo ativo é muito pequeno se comparado ao investimento no mecanismo de proteção. Vide o ponto de inflexão na Figura 08.

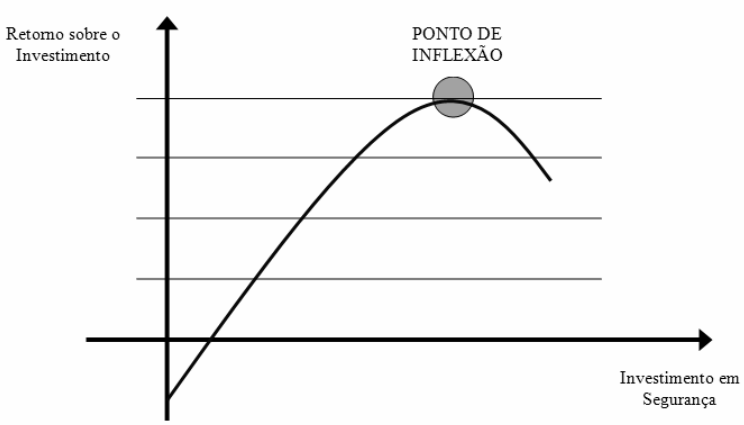


FIGURA 08 – Ponto de inflexão dos investimentos em segurança com relação ao retorno

Segundo Sêmola (2003) a tendência atual é a análise de riscos baseada na comparação da existência ou não de controles de segurança, e não mais somente com o foco principal somente nas vulnerabilidades. Isto devido à ampla aceitação e credibilidade da norma NBR ISO/IEC 17799:2005 no campo da gestão da segurança da informação. Assim, os responsáveis por segurança não precisam trabalhar somente nas vulnerabilidades individualmente, podendo concentrarem-se nos controles propostos pela norma.

2.1.5 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, estudada nesta pesquisa, o COBIT[1], RFCs (*Request for Comments*), etc.

Segundo Sêmola (2003), o universo de controles que podemos aplicar é bem vasto, pois os mecanismos devem cobrir três pontos de segurança: **a humana, a física e a tecnológica.**

No tocante ao *peopleware* (capital humano), os principais controles são os seguintes:

- seminários de sensibilização;
- cursos de capacitação técnica;
- campanhas para divulgar a política de segurança da organização;

[1] Trata-se de uma estrutura para o gerenciamento dos processos de negócios alinhada a um modelo de governança em TI que permite o entendimento e o gerenciamento dos riscos.

- uso de crachás;
- procedimentos padronizados para quando da demissão e contratação de pessoal;
- assinatura de termos de responsabilidade;
- assinatura de termos de confidencialidade;
- sistemas de auditoria; e
- e outros.

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* é o eixo central de todo o sistema para a segurança da informação da corporação. É quem recebe toda a pressão para resultados, e quem é demandado a adequar o nível de controle e o nível de segurança dos ativos da organização. Resumidamente, o *Security Officer* é o responsável por todos os processos inerentes a segurança da informação.

Em virtude das grandes atribuições e responsabilidades que este profissional da segurança tem, ele preferencialmente deve estar no mesmo nível dos executivos da organização. Suas habilidades devem ser:

- possuir conhecimentos e perfil tecnológico, porém deve ser um multiespecialista, tendo uma visão completa e horizontal da segurança da informação;
- saber conduzir projetos;
- coordenar equipes e liderança;
- facilidade de comunicação;
- habilidade para mobilizar pessoas;
- saber trabalhar sob pressão; e
- seriedade e credibilidade entre os colaboradores, executivos e direção da organização.

No que se diz respeito aos aspectos físicos, os mecanismos voltados aos controles de acesso aos ambientes físicos e controles de estados são:

- adoção de roletas;
- climatizadores;
- extintores de incêndio;

- cabeamento estruturado;
- salas-cofre;
- dispositivos de biometria;
- *smartcards*;
- circuito interno de vídeo;
- alarmes e sirenes;
- *nobreaks*;
- dispositivos de armazenamento; e
- etc.

Estes mecanismos de segurança física listados acima, são exemplos de controles implementados e operando para seguir o que recomenda a NBR ISO/IEC 17799:2005 em seu capitulo 9 "Segurança Física e do Ambiente", onde os objetivos principais dos controles do capitulo 9 da norma são: prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações; e impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades.

Já no que diz respeito aos aspectos tecnológicos a lista de mecanismos aplicáveis é extensa, pois além da diversidade e heterogeneidade de tecnologias, ainda deve-se considerar a rapidez com que o setor nos apresenta uma nova ferramenta ou equipamento, pois a diversidade de ataques e ameaças se renova e se multiplica a cada dia.

Pode-se verificar nas Figuras 09 e 10 os mecanismos de controles mais utilizados e uma perspectiva para implementações futuras, conforme a 9ª Pesquisa Nacional de Segurança da Informação realizada no ano de 2003 pela empresa Módulo Security.

Medidas Implementadas em 2003

Ranking	*2003*	*%*
1º	Antivírus	90,0%
2º	Sistema de backup	76,5%
3º	Firewall	75,5%
4º	Política de Segurança	72,5%
5º	Capacitação Técnica	70%
6º	Software de controle de acesso	64%
7º	Segurança física na sala de servidores	63%
8º	Proxy server	62%
9º	Criptografia	57%
10º	Análise de riscos	56%

FIGURA 09 – Os 10 mecanismos de segurança mais implementados
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003
Obs.: o total é superior a 100% devido as múltiplas respostas

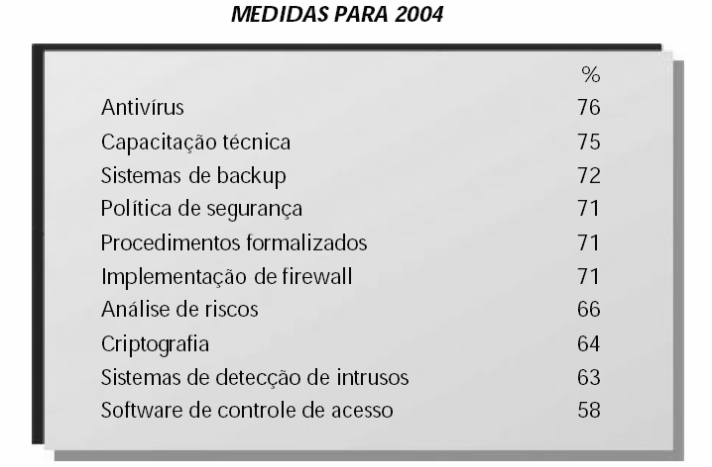


FIGURA 10 – Previsão das medidas a serem implementadas em 2004
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003
Obs.: o total é superior a 100% devido as múltiplas respostas

Abaixo se discorre sobre algumas ferramentas para sistemas e segurança da informação para a área de tecnologia:

- **antivírus -** software capaz de detectar e eliminar vírus de computador, assegurando a integridade e disponibilidade das informações;
- **backup -** sistema que possibilita a reprodução e a posterior restauração de informações a partir de meios de armazenamento;
- **firewall -** sistema baseado em software ou hardware capaz de controlar o acesso entre duas redes ou sistemas, impedindo acessos indevidos e ataques. Também pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre sua rede e a Internet, o seu principal objetivo é permitir somente a transmissão e a recepção de dados autorizados;
- **proxy - s**ão usados para permitir aos micros de uma rede interna o acesso a Web, FTP e outros serviços, no qual ele foi previamente configurado. O proxy é um servidor especial, que encontra-se em um computador que comumente também pode agir um *Firewall*, escondendo os computadores da rede interna. O servidor proxy recebe requisições de máquinas da rede interna, envia aos servidores que estão do lado externo da rede, lê as respostas externas e envia de volta o resultado aos clientes da rede interna;
- **roteadores**: são mecanismos do nível de rede, de software ou de hardware, que usam uma ou mais métricas para decidir sobre o melhor caminho para a

transmissão de tráfego da rede. Alguns dos roteadores, além de executar a sua função, têm desempenhado o papel de um *Firewall*;

- **zona desmilitarizada (DMZ) -** trata-se de um barramento de rede independente que não tem acesso ao barramento da rede local onde estão outros servidores e estações que não podem ser acessados da Internet;
- **criptografia -** é uma ciência que estuda e aplica meios e métodos para proteger a confidencialidade das informações através da codificação ou cifração da mensagem que permite a restauração da informação original através do processo de descodificação. Aqui são amplamente utilizados algoritmos matemáticos e de criptoanálise para maior ou menor segurança conforme a complexidade da informação;
- ***virtual private network* (VPN) -** sistema implementado por software ou hardware capaz de assegurar uma conexão de dados segura em meios públicos (como a Internet) através de mecanismos de tunelamento, autenticação e criptografia;
- ***intrusion detection system* (IDS) - s**istema capaz de identificar a atividade de um invasor na rede e iniciar procedimentos de aviso. Existem diversos tipos de ferramentas IDS para diferentes plataformas, porém as ferramentas IDS trabalham basicamente de modo parecido, ou seja, analisando os pacotes que trafegam na rede e comparando-os com assinaturas já prontas de ataques, identificando prováveis anomalias ou ataques que possam vir a ocorrer em sua rede; e
- **esteganografia -** é uma técnica que propõe a inclusão de informações confidenciais em arquivos aparentemente normais e que só podem ser extraídas pelo destinatário que possui o mapa de camuflagem. A vantagem que por não ser criptografada pode passar despercebida por aqueles que possuem a intenção de roubar informações.

2.1.6 Política de Segurança da Informação

Segundo a RFC 2828 (2002), a Política de Segurança é um conjunto de regras e práticas que regulam como um sistema ou uma organização disponibilizará serviços seguros, com a finalidade de proteger os recursos críticos e os principais ativos da organização.

A norma NBR ISO/IEC 17799:2005 no seu capítulo 5 cita que um dos objetivos da política de segurança é prover uma orientação e o apoio da direção da organização para a

segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

Conforme abordado por Sêmola (2003), devido a sua importância a política de segurança pode ser comparada a constituição federal para um país, assumindo grande abrangência e podendo ser subdividida em três partes: *diretrizes*, *normas* e *procedimentos,* conforme ilustra a Figura 11.

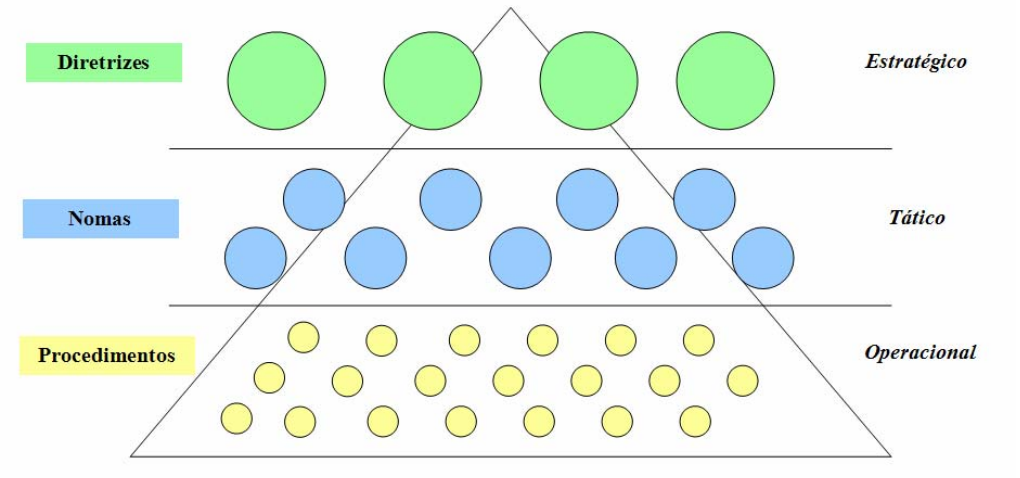


FIGURA 11 – Partes da Política de Segurança conforme seu nível na pirâmide da organização

As diretrizes estão num nível estratégico e precisam dimensionar a importância que a organização dá para sua informação, além de esclarecer todo o seu comprometimento em apoiar e aplicar a segurança da informação. Já, as normas, no nível tático, detalham situações, ambientes e processos específicos, fornecendo orientações para o uso adequado dos ativos. Por fim, os procedimentos, no nível operacional, deverão estar presentes na política em maior ou menor quantidade por perfil profissional, dando uma descrição minuciosa de cada ação a ser realizada.

É de suma importância o envolvimento da direção na construção e aceitação da política, refletida pelo caráter oficial com que a política é divulgada e comunicada a todos dentro da organização. A NBR ISO/IEC 17799:2005 recomenda que o documento da política de segurança da informação seja aprovado pela direção, para esta ser publicada e comunicada a todos os funcionários e partes externas relevantes.

A norma NBR ISO/IEC 17799:2005 afirma que o documento da política de segurança da informação da organização contenha declarações relativas a:

a) uma definição de segurança da informação, metas globais, importância da segurança da informação, escopo e outras;
b) uma declaração de comprometimento e apoio da direção;
c) uma estrutura para estabelecer os objetivos de controle e os controles;
d) uma pequena explanação das políticas, normas, princípios e requisitos de conformidade de segurança da informação, incluindo: conformidade com legislação e contratos, requisitos de conscientização e treinamento e educação em segurança da informação, gestão de continuidade do negócio, conseqüências das violações da política;
e) definição das responsabilidades gerais e específicas; e
f) referências a documentos que apóiam a política.

É imprescindível de que a política de segurança da organização receba revisões temporais e/ou orientada a eventos que ocasionem mudanças significativas. Ou seja, faça-se uma análise crítica, incluindo avaliação de oportunidades de melhoria tendo como meta gerenciar a segurança da informação em resposta às mudanças no ambiente, circunstâncias de negócios, leis ou ambiente técnico.

2.1.7 Solução de Segurança da Informação

Para uma correta gestão da segurança da informação, a participação de todos os colaboradores da organização se faz necessária. Conforme o processo do negócio, tamanho ou complexidade da organização pode ser que seja necessária a participação de acionistas, fornecedores, clientes, e possivelmente também o auxilio de uma consultoria externa (NBR ISO/IEC 17799:2005).

A NBR ISO/IEC 17799:2005 retrata que a solução para a segurança da informação é implementação de um conjunto de controles adequados, onde lista-se política, procedimentos, estruturas organizacionais e funções de software e hardware.

A norma NBR ISO/IEC 17799:2005 recomenda que se estabeleçam os requisitos da segurança da informação por meio da análise/avaliação de riscos; legislações vigentes, estatutos, portarias, etc.; e conjuntos particulares de princípios e requisitos para o processamento da informação da organização.

Na análise/avaliação de riscos os gastos com os controles precisam ser balanceados, assim pode-se utilizar um estudo de ROI.

Uma vez que os requisitos de segurança e os riscos foram levantados convém que controles apropriados sejam selecionados e implementados para assegurar os níveis de risco a patamares aceitáveis (NBR ISO/IEC 17799:2005).

2.1.8 Fatores Críticos de Sucesso

A norma NBR ISO/IEC 17799:2005 retrata que existem fatores que podem influenciar favoravelmente o sucesso de um projeto de segurança da informação dentro de uma organização.

Abaixo se descrevem alguns destes fatores críticos abordados pela NBR:

- a existência de uma Política de Segurança da Informação, em consonância com os objetivos do negócio, já consta como um fator extremamente colaborador;
- a Política de Segurança da Informação, só será aceita e respeitada se houver o comprometimento e apoio visível de todos os níveis gerenciais. A mesma Política deve ser eficientemente divulgada para todos os colaboradores, independentemente do nível hierárquico, para que se possa alcançar a conscientização almejada;
- em algum momento será necessária a provisão de recursos financeiros para as atividades de Gestão da Segurança da Informação;
- realização de um 'plano' de conscientização, onde será oferecido treinamento, educação, nivelamento de conhecimento sobre segurança, ratificação da importância da segurança da informação, divulgação das normas e diretrizes sobre a política de segurança da informação; e
- o estabelecimento de um eficiente processo de gestão de incidentes, também é um fator importante.

A norma considera esses fatores como críticos para o sucesso da implementação da segurança da informação.

2.2 Normalizações

Segundo Holanda (2006), as normas são criadas para estabelecerem diretrizes e princípios para melhorar a gestão de segurança nas empresas e organizações. Ariosto Farias Jr., delegado do Brasil no Comitê Internacional da ISO/IEC 17799, em entrevista para revista

Modulo Security Magazine disse acreditar que uma das explicações para a tendência de adoção de normas é que cada vez mais no mundo dos negócios percebe-se a importância de se proteger as informações, além do fato de que a informação é um ativo essencial para os negócios de qualquer organização.

No atual cenário brasileiro, todos os acontecimentos na área de segurança não têm impactado em mudanças ou transformações profundas na área de segurança da informação corporativa. Com as discussões e projetos internacionais e até mesmo os nacionais, há muito tempo vêm ocorrendo e surgindo dentro das organizações uma preocupação maior das pessoas envolvidas, no sentido de como e quais serão as diretrizes de segurança para se alcançar, coletar, solicitar, acessar, trocar, manipular um de seus principais patrimônios: as informações que deverão circular na instituição (CASSANAS, 2006).

Conforme Rocha (2006) dois bons guias para o gestor de segurança da informação, ou *security officer* das diversas organizações, são as normas BS 7799 e a ISO/IEC 17799. Ambas proporcionam ao profissional de segurança da informação os subsídios necessários para uma boa gestão. No Brasil a norma NBR ISO/IEC 17799:2005 cumpre esta função.

2.3 A Norma NBR ISO/IEC 17799:2005

Segundo Rocha (2005), existe várias normas na área de segurança da informação em diversos países, porém há um consenso mundial que a norma ISO/IEC 17799 é o melhor código de prática em gestão da segurança da informação que existe no mercado. Nenhuma outra norma tem tamanha abrangência, pois a ISO/IEC 17799 foi atualizada e melhorada por um grupo de mais de cinqüenta especialistas de todas as partes do mundo, inclusive o Brasil.

A 9ª Pesquisa Nacional de Segurança da Informação realizada pela empresa Módulo Security em 2003, nas questões de legislações, normas e regulamentações de segurança que norteiam as organizações, aponta a norma ISO 17799 como o referencial mais utilizado entre os pesquisados (vide Figura 12).

Conforme Duarte (2006), o Brasil foi o primeiro país no mundo a traduzir a ISO/IEC 17799:2005 para sua língua e publicou-a oficialmente como norma nacional em setembro de 2005 com a denominação de NBR ISO/IEC 17799:2005.

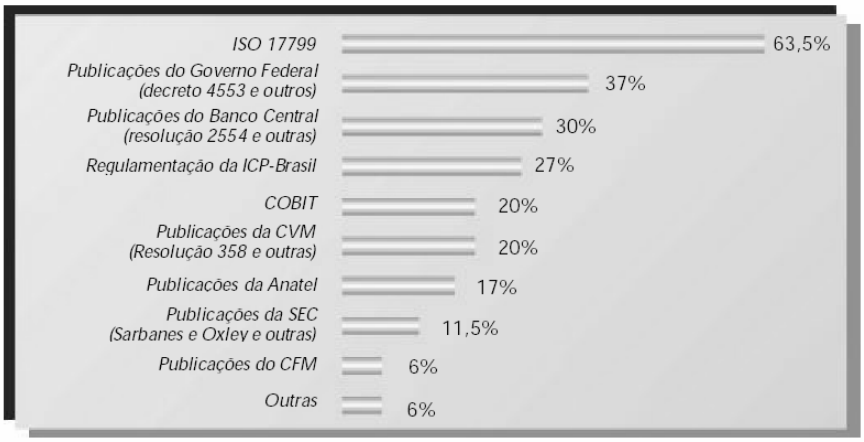


FIGURA 12 – Principais regulamentações/normas utilizadas
Fonte: 9ª Pesquisa Nacional de Segurança da Informação, Modulo Security 2003
Obs.: o total é superior a 100% devido as múltiplas respostas

Os principais benefícios que se pode obter com a adoção da norma NBR ISO/IEC 17799:2005 são: proteção das informações e ativos sensíveis da organização às ameaças e vulnerabilidades, continuidade dos negócios, aumento da competitividade, atendimento aos requisitos legais, manutenção e aumento da reputação e imagem da instituição.

Outra grande importância da norma encontra-se na vantagem de que seu uso ou aplicação permite a uma empresa ou organização a construção de forma ágil de uma política de segurança da informação baseada em controles de segurança eficientes.

2.3.1 Origem

A ISO/IEC 17799 remonta de 1987, quando o Departamento de Comércio e Indústria do Reino Unido *(UK Department of Trade and Industry - DTI)*, com a necessidade de criar um plano para proteção das informações do Reino Unido, criou o Centro de Segurança de Computação Comercial *(Commercial Computer Security Center - CCSC)*. Este centro tinha como uma de suas finalidades, a criação de uma norma de segurança das informações para as empresas britânicas.

Em 1989 o CCSC criou um guia de segurança para usuários, o PD0003 – um Código de Práticas para Gerenciamento de Segurança da Informação *(a Code of Practice for Information Security Management)*. Após ter sido disponibilizada para consulta pública, foi desenvolvido pelo Padrão Britânico *(British Standard)* em 1995, uma versão final deste documento, a BS 7799:1995.

A BS 7799 é formada por três partes:

- BS 7799-1: *Code of practice for information security management*;
- BS 7799-2: *Information Security Management Systems - Specification with guidance for use; e*
- BS 7799-3: *Guidelines for information security risk management*.

Depois de melhorias na BS 7799, ela foi submetida à Organização Internacional para Normalização *(International Organization for Standartization – ISO)* para se tornar um padrão internacional. Em dezembro de 2000, a BS 7799 foi aceita como um padrão internacional pelos países membros da ISO, do qual o Brasil faz parte, com a denominação de ISO/IEC 17799:2000. A junção das siglas ISO com IEC *(International Engineering Consortium)* se deve ao esforço destas duas organizações em produzir normas internacionais.

No mesmo ano a Associação Brasileira de Normas Técnicas (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. No segundo semestre de 2005 foi lançada a nova versão da norma a **NBR ISO/IEC 17799:2005**.

Conforme traz a própria NBR ISO/IEC 17799:2005 no seu prefácio, ela foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01) e é considerada equivalente à ISO/IEC 17799:2005.

A NBR também traz informações de que uma nova família de normas de sistema de gestão de segurança da informação encontra-se em desenvolvimento. Esta família incluirá normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes de implementação. O esquema de numeração será a série de números em seqüência 27000.

A partir do ano de 2007, uma nova edição da ISO/IEC 17799 fará parte do novo esquema de numeração como ISO/IEC 27002, conforme pode ser verificado na Figura 13. Entretanto, até o presente momento, tal norma ainda não foi publicada.

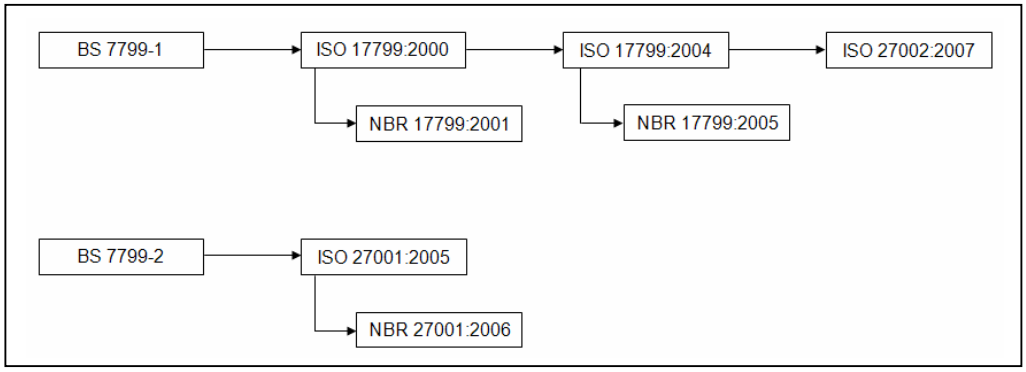


FIGURA 13 – Genealogia das Normas de Segurança da Informação tipo NBR

2.3.2 Escopo da norma

O objetivo principal da norma é orientar, e a partir disto criar uma sinergia entre as diferentes corporações que estão diante do desafio de gerenciar a segurança da informação. Todas as versões da norma, inclusive a brasileira, tratam os aspectos de forma bem abrangente, porém sempre girando em torno do eixo: **confidencialidade**, **integridade** e **disponibilidade.**

A NBR ISO IEC 17799:2005, como o próprio título já diz, é um código de prática de gestão para segurança da Informação, e sua importância pode ser dimensionada pelo número cada vez maior de ameaças que as informações e os ativos estão expostos.

Os objetivos explícitos desta norma são:

- Estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em organizações;
- Os controles da norma têm como objetivos serem implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos;
- Aumentar, se implementada, a confiança nas atividades inter-organizacionais.

Em seu texto a NBR ISO/IEC 17799:2005 aborda 11 tópicos, abaixo relacionados:

- **1. Política de Segurança da Informação -** Este tópico descreve a importância e aponta os principais assuntos que devem ser abordados numa política de segurança;
- **2. Segurança Organizacional -** Este tópico aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços;

- **3. Gestão de Ativos** - Este tópico trata da classificação, o registro e o controle dos ativos da organização;
- **4. Segurança em Recursos Humanos** - Neste tópico são abordados a inclusão de responsabilidades relativas a segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados a segurança;
- **5. Segurança Física e Ambiental** - Este tópico aborda a necessidade de um controle de acesso físico, necessidade de proteger equipamentos e a infra-estrutura de tecnologia de Informação;
- **6. Gestão das Operações e Comunicações** - Esta seção aborda as principais áreas que devem ser objeto de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras;
- **7. Controle de Acesso** - Este tópico aborda o controle de acesso a sistemas, a definição de competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos;
- **8. Sistemas de Informação** - Neste item são abordados os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos e segurança do desenvolvimento e suporte de sistemas;
- **9. Gestão de Incidentes de Segurança** - Notificação de fragilidades e eventos de segurança da informação e Gestão de incidentes de segurança da informação e melhorias;
- **10. Gestão da Continuidade do Negócio** - Esta seção reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado; e
- **11. Conformidade -** A seção final aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes.

Na Tabela 02 apresenta-se, os respectivos capítulos da norma com os seus respectivos objetivos a serem atingidos quando da sua aplicação.

TABELA 02 – Capítulos da Norma NBR ISO/IEC 17799:2005 e objetivos

Cap.	Abrangência	Objetivos
0	**Introdução**	• Contextualizar a Segurança da Informação.
1	**Objetivo**	• Explicar a finalidade da Norma.
2	**Termos e Definições**	• Conceituar o significado dos termos e definições contido na Norma.
3	**Estrutura da Norma**	• Mostrar a estrutura e quais são os tópicos da Norma.
4	**Análise/avaliação e Tratamento de Riscos**	• Explicar o que vem a ser Análise/avaliação e Tratamento de Riscos de Segurança da Informação.
5	**Política de Segurança da Informação**	• Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.
6	**Organizando a Segurança da Informação**	• Gerenciar a segurança da informação dentro da organização; • Manter a segurança dos recursos de processamento da informação e das informações da organização acessadas por partes externas.
7	**Gestão de Ativos**	• Alcançar e manter a proteção adequada dos ativos da organização; • Assegurar que a informação receba um nível adequado de proteção.
8	**Segurança em Recursos Humanos**	• Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos; • Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.
9	**Segurança Física e do Ambiente**	• Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização; • Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização.
10	**Gestão das Operações e Comunicações**	• Garantir a operação segura e correta dos recursos de processamento da informação; • Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados; • Minimizar o risco de falhas nos sistemas; • Proteger a integridade do *software* e da informação; • Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação; • Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte; • Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio; • Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas; • Garantir a segurança de serviços de comércio eletrônico e sua utilização segura; • Detectar atividades não autorizadas de processamento da informação.

11	**Controle de Acesso**	• Controlar o acesso à informação; • Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; • Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; • Prevenir acesso não autorizado aos serviços de rede; • Prevenir acesso não autorizado aos sistemas operacionais; • Prevenir acesso não autorizado à informação contida nos sistemas de aplicação; • Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.
12	**Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**	• Garantir que segurança é parte integrante de sistemas de informação; • Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; • Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; • Garantir a segurança de arquivos de sistema; • Manter a segurança de sistemas aplicativos e da informação; • Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
13	**Gestão de Incidentes de Segurança da Informação**	• Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil; • Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.
14	**Gestão da Continuidade do Negócio**	• Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.
15	**Conformidade**	• Evitar violação de quaisquer obrigações legais, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação; • Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação; • Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

Fonte: NBR ISO/IEC 17799:2005 com adaptações do autor.

2.3.3 Dos Controles de Segurança

Para a Norma NBR ISO/IEC 17799:2005, uma vez que os requisitos de segurança tenham sido estabelecidos, os riscos tenham sido identificados, as decisões de como tratar os riscos tenham sido definidas, é essencial a escolha e a implementação dos controles adequados, para que os riscos caiam a um patamar aceitável e definido pela organização.

Embora todos os controles elencados na Norma sejam importantes, a real aplicabilidade de qualquer controle deve estar relacionada aos riscos específicos que a organização está exposta. Se o risco é alto mas o impacto é reduzido, talvez não seja o caso de

se elevar as medidas de segurança. Medidas de segurança normalmente implicam em elevação de custos, dado que o que de fato importa são as conseqüências (impactos) da quebra de segurança, logo nem sempre são relevantes. Às vezes é mais vantajoso correr riscos do que disponibilizar uma grande quantidade de recursos para diminuir o risco de sua ocorrência. Os gastos com a implementação de controles de segurança precisam ser balanceados de acordo com os danos causados pelas potenciais falhas na segurança.

Este balanceamento é obtido com a análise de riscos e o estudo de ROI, mais especificamente neste trabalho, com a Matriz de Análise de Riscos, pois na análise de riscos é possível identificar a necessidade ou não da adoção de medidas de segurança ou implementação dos controles.

A Figura 14 mostra um exemplo de controle da norma NBR ISO/IEC 17799:2005 e dos níveis que os mesmos podem assumir.

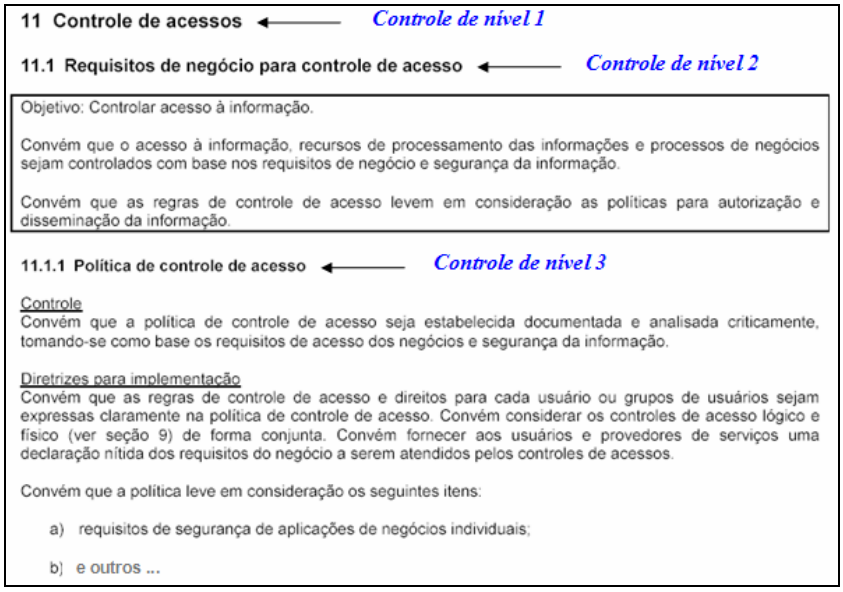


FIGURA 14 – Níveis dos controles da NBR ISO/IEC 17799:2005
Fonte: NBR ISO/IEC 17799:2005

Os controles a serem aplicados devem sempre cumprir a finalidade de se reduzir os riscos a um nível aceitável e previamente definido pela organização (HOLANDA, 2006).

Os controles indicados pela NBR ISSO/IEC 17799:2005 estão listados no Anexo A. Entretanto, deve-se ter em mente que indubitavelmente nenhum conjunto de controles, por mais abrangentes que seja, alcançará 100% de segurança.

2.3.4 Certificação

Muitas são as discussões sobre os diferentes métodos e modelos de gestão de segurança da informação (BORGES, 2003). Assim, aumentam as adesões aos mandamentos de segurança corporativa. Profissionais envolvidos com certificações acreditam que a tendência da NBR ISO/IEC 17799 é seguir os mesmos passos das certificações de qualidade mais famosas, como a ISO 9000.

Entende-se por certificação um conjunto de atividades realizadas por organismos, independentes da relação comercial, com o objetivo de atestar publicamente, que determinada organização possui produto, processo ou serviço de acordo com os requisitos especificados por norma ou legislação.

A ABNT recomenda que para se obter a certificação numa determinada norma, a organização deve seguir os seguintes passos:

1. Aquisição da Norma;
2. Estudo e interpretação da Norma;
3. Implementação da Norma;
4. Solicitar a ABNT a avaliação; e
5. Certificação.

Segundo Borges (2003), os principais benefícios de uma certificação bem sucedida, dizem respeito à percepção dos colaboradores em relação à importância de preservar os ativos de informação e dar o tratamento adequado a dados importantes e sigilosos, muitas vezes trazendo mais pontos positivos para a organização do que a obtenção do certificado.

Para se obter uma certificação na BS 7799-2 é preciso definir um Sistema de Gestão de Segurança da Informação (SGSI). Conforme Donner (2006), o real valor de possuir uma certificação em BS 7799-2, ou na nova ISO 27001:2005, é a obtenção da chamada **cultura da segurança** pela organização. Pois para se obter esta certificação, vários são os requisitos que a organização deve obedecer, por exemplo:

- o nível de comprometimento e investimentos requer esforços bem direcionados de dirigentes e colaboradores de toda organização;
- é necessário desenvolver projetos de segurança, mapear processos, estabelecer diretrizes e procedimentos, conformidade com as normas, análise de riscos, análise de impactos, planos de continuidade e recuperação de desastres, normas, regulamentos e políticas de segurança; e

- ter padronização de processos e documentação, bem como auditorias periódicas.

Treinamento em Segurança da Informação e divulgação da Política de Segurança para todas as pessoas da organização, também é de suma importância que aconteça para que a cultura em segurança da informação se estabeleça.

Segundo o *International ISMS Register*, o Brasil possui atualmente 15 organizações certificadas em BS 7799-2:2002 ou ISO/IEC 27001:2005, e encontra-se em 18° posição dentre os paises que possuem organizações certificadas, e em primeiro lugar na América Latina, conforme demonstrado na Tabela 03 (ISMS, 2007).

TABELA 03 – Número de organizações certificadas por País.

Japão	2043	Austria	11	*Oman*	2
Reino Unido	329	Arábia Saudita	9	Paquistão	2
Índia	285	Espanha	9	*Slovak Republic*	2
Taiwan	127	Filipinas	8	África do Sul	2
Alemanha	74	Suécia	8	*Sri Lanka*	2
Hungria	57	*UAE*	8	Armênia	1
Coréia	49	Islândia	7	Bulgária	1
EUA	48	Grécia	5	Gibraltar	1
China	47	Kuwait	5	Egito	1
Itália	43	Federação Russa	5	Líbano	1
Austrália	42	Tailândia	4	Lituânia	1
Países Baixos	31	Argentina	3	Luxemburgo	1
Singapura	28	Barém	3	Macedônia	1
Hong Kong	26	Canadá	3	*Moldova*	1
República Tcheca	25	Croácia	3	Morocos	1
Malásia	19	França	3	Nova Zelândia	1
Polônia	17	Indonésia	3	Peru	1
Brasil	**15**	*Isle of Man*	3	Quatar	1
Ireland	15	Macau	3	Sérvia e Montenegro	1
Suíça	15	Romênia	3	Ucrânia	1
Finlândia	14	Eslovênia	3	Uruguai	1
Noruega	14	Bélgica	2	Vietnã	1
Turquia	13	Colômbia	2	**Total Absoluto**	**3530**
México	12	Dinamarca	2		

Fonte: *International ISMS Register* (http://www.iso27001certificates.com)

Pode-se observar na Tabela 03 que o Japão e o Reino Unido (Inglaterra) são os países com o maior número de empresas certificadas no mundo. O grande número de certificações que as organizações japonesas possuem se explica devido ao Japão no passado já possuir uma metodologia de certificação em Sistemas de Gestão da Segurança da Informação, com a disseminação da norma BS:7799-2, este país passou a adotar esta norma como base para certificações. Já no caso da Inglaterra, é que a mesma é possuidora de grande tradição em relação à certificações de Sistemas de Gestão, seja ela da qualidade, do meio ambiente, da saúde, segurança ocupacional ou segurança da informação. A Inglaterra lidera mundialmente o número de empresas certificadas na ISO 9001, além da BS-7799-2 ser britânica.

É importante salientar que a norma NBR ISO/IEC 17799:2005 encontra-se perfeitamente alinhada com o que preconiza a BS-7799-2 e a ISO/IEC 27001:2005 (normas certificadoras), assim pode-se dizer que o estudo e a implementação desta norma pode ser um primeiro passo rumo a correta gestão da segurança da informação e uma futura certificação para uma organização.

2.4 Trabalhos Correlatos

No portal da CAPES (Coordenação e Aperfeiçoamento de Pessoal de Nível Superior, disponível em http://www.capes.gov.br) pesquisas feitas com as expressões “segurança da informação” e “17799” mostraram que existem muitos trabalhos e estudos com relação a segurança da informação de forma mais ampla, e com relação a norma ISO/IEC 17799 a literatura disponível é mais restrita. Vale ressaltar que a pesquisa avançada feita no portal da CAPES somente fornecia opção de busca até o ano de 2004, não nos possibilitando buscas nos anos de 2005 e 2006.

No site da empresa Modulo Security (http://www.modulo.com.br) conforme pesquisa geral no site com as expressões “segurança da informação” e “17799”, encontrou-se para a primeira expressão 5.458 trabalhos, pesquisa e artigos, já para a segunda expressão encontramos 113. No link “Trabalhos Acadêmicos” encontravam-se disponibilizados com relação direta a expressão “17799” 02 trabalhos no ano de 2005 e 03 trabalhos no ano de 2006. No mesmo link a expressão “segurança da informação” trouxe 06 trabalhos no ano de 2002, 10 trabalhos no ano de 2003, 05 trabalhos no ano de 2004, 09 trabalhos no ano de 2005 e 04 trabalhos no ano de 2006.

No portal da **Biblioteca Digital de Teses e Dissertações (BDTD)**[2] em http://bdtd.ibict.br/bdtd/, em buscas com a expressão "17799", encontrou-se 04 (quatro) pesquisas, uma do ano 2002, duas do ano de 2003 e uma do ano de 2006. Com relação à palavra-chave "segurança da informação" foram encontrados mais trabalhos com relação a estes assuntos, haviam 10 trabalhos disponibilizados no site, que foram realizados entre os anos de 2002 e 2006.

As dissertações encontradas nos sites citados anteriormente, e que mais tem relação com segurança da informação e a NBR ISO/IEC 17799 foram:

- MACHADO, César de Souza. Gerenciamento da Segurança da Informação no Teletrabalho. Dissertação de Mestrado - Universidade Federal de Santa Catarina, Florianópolis, 2002.
- GABBAY, Max Simon. Fatores Influenciadores da Implementação de Ações de Gestão de Segurança da Informação: um estudo com Executivos e Gerentes de Tecnologia da Informação em empresas do Rio Grande do Norte. Dissertação de Mestrado – Universidade Federal do Rio Grande do Norte, Natal, 2003.
- CAVALCANTE, Sayonara de Medeiros. Segurança da Informação no Correio Eletrônico baseada na ISO/IEC 17799: um estudo de caso em uma instituição de ensino superior, com foco no treinamento. Dissertação de Mestrado – Universidade Federal do Rio Grande do Norte, Natal, 2003.
- FILHO, Ramiro Fernandes Rodrigues. Proposta de Metodologia para a Elaboração de um Plano Diretor de Segurança da Informação. Dissertação de Mestrado – Faculdades IBMEC, Rio de Janeiro, 2005.
- LIMA, Luiz Fernando Ferreira de Medeiros. Percepção de Segurança em Sistemas de Informação e sua relação com a qualidade percebida de Serviços, Perfil de Liderança e Perfil dos Seguidores, entre as Diretorias do INMETRO. Dissertação de Mestrado Profissional em Sistemas de Gestão – Universidade Federal Fluminense, Niterói, 2006.

---

[2] O Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) www.ibict.br do Ministério da Ciência e Tecnologia coordena o projeto da **Biblioteca Digital de Teses e Dissertações (BDTD)**, que busca integrar os sistemas de informação de teses e dissertações existentes nas Instituições de Ensino Superior (IES) brasileiras, bem como estimular o registro e a publicação de teses e dissertações em meio eletrônico.

Outros trabalhos também relevantes, encontrados nos periódicos da CAPES, particularmente no que se refere a segurança da informação em instituições de ensino e utilização da norma ISO/IEC 17799:2005 são:

- MAY, Lauren and LANE, Tim. A Model for Improving e-Security in Autralian Universities. Journal of Theoretical and Applied Eletronic Commerce Research. v 1, p. 90-96, 2006.
- BAKRY, Saad Haj., SALEH, Mohammad S. and ALRABIAH, Abdullah. Using ISO 17799:2005 information security management: a STOPE view with six sigma approach. International Journal of Network Management – 2007. v 17, p. 85-97, jun 2006.

O trabalho de Machado (2002), apresenta um estudo sobre a segurança da informação em sistemas de teletrabalho e teve como objetivo subsidiar o gerenciamento da segurança da informação. Para tal, uma pesquisa foi realizada para verificar como as empresas brasileiras estão administrando seus programas de teletrabalho com relação à segurança da informação. Com base na fundamentação teórico-empírica e nos resultados da pesquisa, foi estruturada uma metodologia baseada em um modelo de segurança para garantir a confidencialidade das informações em sistemas de teletrabalho. Partindo-se de um contexto de acesso remoto – uma atividade meio – o modelo delineado, implementado por meio de ferramentas e controles desenvolvidos a partir da norma ISO/IEC 17799, focaliza a atividade fim – a realização do teletrabalho. Os resultados obtidos, por meio da aplicação do modelo em uma situação real, permitiram validar a aplicação da metodologia proposta como um instrumento efetivo para o gerenciamento da segurança das informações, atendendo de forma rápida e eficiente as necessidades de empresas e teletrabalhadores.

Gabay (2003) apresenta em sua dissertação resultados descritivos de uma pesquisa que identificou quais os fatores que influenciaram os executivos e gerentes de TI nas suas percepções em relação a segurança da informação. Neste trabalho também foram levantados os perfis das empresas e dos executivos e gerentes de TI do estado do Rio Grande do Norte e aferiu o nível de concordância dos respondentes em relação a norma NBR ISO/IEC 17799 somente na dimensão controle de acesso. A pesquisa concluiu que as empresas no Rio Grande do Norte apresentam baixo nível de conformidade com a referida norma, e que a percepção da segurança da informação dos profissionais envolvidos está diretamente ligada ao tamanho do parque de informática das organizações bem como ao número de ataques sofridos.

A pesquisa de Cavalcante (2003) descreve o resultado de uma pesquisa que objetivou demonstrar a importância que o treinamento do usuário tem sobre a política de segurança das organizações, demonstrando os resultados através de um estudo de caso feito em uma instituição de ensino superior do Estado do Rio Grande do Norte. Todo seu trabalho teve como guia a NBR ISO/IEC 17799, onde se construiu uma política de segurança da informação para o serviço de correio eletrônico. Todo trabalho foi realizado com base em respostas de questionário e entrevistas junto à gerência de informática da instituição de ensino.

Filho (2005) propôs um método para estruturação do planejamento de segurança da informação para uma empresa contemplando e respeitando as particularidades de sua estrutura organizacional e seus objetivos estratégicos. O método apresentou uma metodologia para implementação de um Plano Diretor de Segurança da Informação, com muitas etapas e ferramentas semelhantes ao proposto em (SEMOLA 2003), finalizado com a estruturação do plano.

A dissertação de Lima (2006), foi um estudo de caso, onde se procurou estudar os problemas de incidentes de segurança da informação dentro do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO), no âmbito de suas diretorias e a relação desses índices com a percepção da qualidade dos serviços dos sistemas de informação, com o perfil de liderança e com o perfil dos seguidores. Para esse estudo foram utilizados como referenciais teóricos, a Norma ABNT NBR ISO/IEC 17799, para a gestão da segurança da informação; os modelos conceituais de Parasuraman (1990), para analisar a qualidade percebida dos serviços de informática; os conceitos de Kouzes e Posner (2003), para o perfil de liderança; e os de Kelley (1993), para o perfil dos seguidores. A metodologia da pesquisa foi baseada no método hipotético-dedutivo de Popper (1975).

Segundo May (2006), as universidades têm notado um aumento nas iniciativas de *e-business*, *e-commerce* e *e-learning*, e consequentemente uma correta gestão de segurança se faz necessária. Ele retrata a importância da difusão da cultura da segurança da informação, onde envolve uma mudança de comportamento em toda a organização, e não fazer como muitas organizações fazem, ou seja, a segurança da informação em universidades tende a ser delegada a um escritório do departamento de TI, geralmente "escondido", e sob supervisão de uma pessoa com responsabilidade operacional de segurança e não de gerência. O estudo é baseado em universidades Australianas, e voltado para universidades.

May (2006) propõe um modelo de gestão dividido em cinco camadas: *Contextual Layer, Conceptual Layer, Construct Layer, Physical Layer e Operational Layer*. Estas cinco

camadas do processo são alimentadas por influências externas e internas, e o processo sofre melhorias continuas através do ciclo PDCA *(Plan, Do, Check, Action)*. A proposta do modelo de gestão de May (2006) é diferente do que simplesmente implementar um conjunto de controles, este modelo tenta descrever "como" implementar e não "o que" implementar. É ressaltado na pesquisa também, que a responsabilidade da segurança não pode ficar relegada a somente uma pessoa, ou um setor, e sim uma ação de adoção de padrões em todos os níveis e setores.

Bakry (2006), descreve o uso da norma ISO 17799:2005, integrando suas partes e seus controles dentro dos domínios de "estratégia, tecnologia, organização, pessoas e meio ambiente", ou seja, o chamado *STOPE view (strategy, technology, organization, people, and environment)* (BAKRY, 2001), conforme pode ser visualizado na Tabela 04.

TABELA 04 – Modelo STOPE e a ISO/IEC 17799:2005

STOPE	**Capítulos da ISO/IEC 17799:2005**
Strategy	*5 – Information Security Policy*
Technology	*10 – Communication and Operations Management* *11 – Access Control* *12 – Information Systems Acquisition, Development and Maintenance*
Organization	*6 – Organization of Information Security* *7 – Asset Management* *13 – Information Security Incident Management* *14 – Business Continuity Security*
People	*8 – Human Resources Security*
Environment	*9 – Physical and Environment Security* *15 – Compliance*

Para que o processo possua uma melhoria contínua, Bakry (2006) propõe a utilização da ferramenta *six sigma* (PYZDEK, 2003). O *six sigma* é um processo cíclico que pode ser abreviado por DMAIC, ou seja, *define* (definir), *measure* (medir), *analyze* (analisar), *improve* (melhorar) e *control* (controlar). O autor descreve que esta ferramenta recomenda para seu sucesso a formação de uma equipe de trabalho, e propõe uma equipe divida em seis partes e níveis diferentes: o presidente da organização (*Leadership*), o vice-presidente (*Champions*), chefe do escritório de segurança da informação (*Master black belt*), supervisor (*Black belt*), técnico em TI (*Green belt*) e usuário (*Staff belt*).

Conforme se pode observar nas pesquisas realizadas, a Segurança da Informação vem sendo aplicada e muito utilizada principalmente nas empresas, bancos, indústrias, órgãos de prestação de serviços; porém de todos os trabalhos pesquisados e encontrados, nenhum retratava a utilização e implementação da Norma NBR ISO/IEC 17799:2005 em colégios para proteção de suas informações digitalizadas.

Pode-se concluir que o número de trabalhos e pesquisas realizadas no campo da Segurança da Informação é bem numeroso, em contrapartida estudos e análises dos pontos mais relevantes por ocasião da adoção da norma NBR ISO/IEC 17799:2005 para gestão da segurança da informação ainda são reduzidos.

2.5 Conclusões Parciais

Neste capitulo foi realizada uma revisão de literatura dos principais tópicos relacionados com segurança da informação e a norma NBR ISO/IEC 17799:2005. Todos os conceitos apresentados encontram-se alinhados com a referida norma.

Foi descrita a importância da utilização das normas para a gestão da segurança da informação, e particularmente foi apresentada uma síntese da norma NBR ISO/IEC 17799:2005 explicando o seu surgimento, mostrando sua estrutura, escopo, e citando os controles trabalhados na norma. Tal conhecimento é fundamental para a norma poder ser aplicada.

Também foram citados trabalhos e estudos realizados por pesquisadores e estudiosos no nosso país utilizando como referencial teórico ou prático a NBR ISO/IEC 17799.

Pode-se observar que há muitos trabalhos relacionados a norma, mas inexiste trabalhos com o foco em Colégios.

3 PROCEDIMENTOS METODOLÓGICOS

Conforme a própria NBR ISO/IEC 17799:2005 cita:

> Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. (NBR ISO/IEC 17799:2005, pág. 1)

Segundo a própria NBR, ela serve como um guia prático para desenvolver procedimentos de segurança da informação e elaborar eficientes práticas de gestão da segurança, a fim de aumentar a confiança nas atividades interorganizacionais.

Esta dissertação possui como objetivo geral avaliar 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 analisar a utilização da norma no gerenciamento de segurança dos recursos de TI do Colégio Militar de Santa Maria.

Assim, para a realização desta pesquisa, este capítulo define uma metodologia que além de ajudar a implementar uma gestão de segurança da informação baseada na NBR ISO/IEC 17799:2005, também apresenta dados que podem ser utilizados para analisar as mudanças na organização por ocasião da aplicação da norma.

Os procedimentos aqui aplicados podem ser sumariamente listados sendo:

- levantar todos os ativos tecnológicos responsáveis pela manutenção da organização e que sustentam a sua operação;
- classificar a importância de cada ativo levantado;
- definir a sensibilidade de cada um deles para o caso da ocorrência da quebra de segurança;
- elaborar a Matriz de Riscos, envolvendo ameaças, vulnerabilidades e impactos, possibilitando uma análise detalhada e propondo uma lista de medidas de segurança e controles a serem implementados; e
- construir a Política de Segurança do Colégio.

A seção 3.1 classifica a pesquisa realizada nesta dissertação, as seções 3.2, 3.3, 3.4, 3.5 e 3.6 que se seguem nesse capítulo procuram demonstrar todos os passos executados para a realização dessa pesquisa científica, bem como cada passo para implementação da norma no CMSM.

3.1 Classificação da Pesquisa

Demo (1996, p.34) insere a pesquisa como atividade cotidiana considerando-a como uma atitude, um "questionamento sistemático crítico e criativo, mais a intervenção competente na realidade, ou o diálogo crítico permanente com a realidade em sentido teórico e prático".

Do ponto de vista da sua *natureza* podemos definir esta pesquisa como sendo **Aplicada**, pois visa gerar conhecimento para aplicação prática dirigida a solução de problemas específicos.

Do ponto de vista da *forma de abordagem do problema* esta pesquisa é **Quantitativa**, porque considera que os dados obtidos podem ser quantificados e classificados.

Do ponto de vista dos *objetivos*, se apresenta de modo **Exploratório,** pois segundo Gil (1999), o modo exploratório visa proporcionar maior familiaridade com o problema com vistas a torná-lo explícito ou a construir hipóteses. Envolve levantamento bibliográfico, levantamento de outras experiências práticas com o problema pesquisado e análise de exemplos.

Em síntese, esta pesquisa é aplicada, quantitativa e exploratória.

3.2 Política de Segurança da Informação

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 as políticas, padrões e procedimentos a serem aplicados aos dados e sistemas corporativos.

A Política de Segurança surge da necessidade de declaração de regras para: o acesso à informação; o uso da tecnologia da organização; e o tratamento, manuseio e proteção de dados e sistemas informacionais.

A Política de Segurança deve ser endossada pela alta administração. Embora o documento deva ter uma abrangência ampla, ele precisa concentrar-se em questões de princípio, deixando de lado os detalhes de implementação. O resultado deve ser um documento claro, conciso e estável de declaração dos objetivos de segurança 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".

A construção da Política deve ser realizada com o que recomenda a NBR ISO 17799:2005 em seu tópico ***5.1.1 Documento da política de segurança da informação (pág. 8)***, ou seja, convém que a política contenha declarações relativas à:

- uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
- uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;
- uma estrutura para estabelecer os objetivos de controle e os controles;
- uma breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo: conformidade com a legislação; requisitos de conscientização, treinamento e educação em segurança da informação; gestão da continuidade do negócio; e conseqüências das violações na política de segurança da informação;
- definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação; e
- referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

A Política de Segurança da Informação deve ser comunicada e divulgada através de toda a organização para os usuários e colaboradores de forma relevante, acessível e de fácil compreensão.

3.3 Levantamento dos Pricipais Ativos

Conforme definido no Capítulo 2, 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.

Neste trabalho, o levantamento dos principais ativos realizar-se-á através de questionamentos e entrevistas junto aos principais gestores, visando a identificação dos principais processos do colégio. Parte-se do princípio de que as atividades de segurança devem ter o foco nos principais processos e nas informações que o alimentam. Vale ressaltar que também se busca identificar as necessidades físicas, tecnológicas e de infra-estrutura para o funcionamento destes processos.

Nesta etapa deve-se atingir o seguinte objetivo:

- ► ter um mapeamento dos principais ativos tecnológicos do colégio.

3.4 Mapeamento da Relevância

Após a identificação dos processos críticos e dos principais ativos, deve-se fazer um mapeamento da relevância de cada um deles, para evitar erros na priorização das atividades.

O mapeamento da relevância de cada ativo, envolve um ou mais gestores de visão corporativa do colégio. Cada gestor deve possuir imparcialidade no momento da ponderação da importância do processo, e deve dar uma relação de peso para importância.

A metodologia aqui a ser aplicada, utilizar-se-á de uma faixa de valores de 1 a 5 para indicar o grau de relevância (vide Tabela 4). Durante a análise, a todo o momento deve ser relembrada a importância do processo-alvo para o colégio, repontuando ao longo da atividade todos os processos.

TABELA 5 – Escala para classificação da relevância

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:SÊMOLA (2003 pag. 91).

A aplicação destes critérios será de forma holística, para subsidiar as demais etapas pelos parâmetros de ponderação utilizados aqui.

Nesta etapa devem-se atingir os seguintes objetivos:

- ► mapeamento da relevância dos principais ativos do colégio; e
- ► envolvimento dos gestores de visão holística do negócio.

3.5 Estudo de Impactos CIDAL e Prioridades GUT

Após a identificação dos ativos na etapa anterior, deve-se realizar 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 será realizado através de entrevista isolada com o gestor do ativo, e o mesmo critério de escala de classificação, utilizado no mapeamento da relevância (Tabela 04), será utilizado aqui, mas sem analisar o todo (vide Tabela 05).

TABELA 6 – Escala para classificação da sensibilidade

ESCALA		**CONCEITOS**			**ASPECTOS**	
Ativo X		CONFIDENCIALIDADE	INTEGRIDADE	DISPONIBILIDADE	AUTENTICIDADE	LEGALIDADE
1	**Não Considerável**					
2	**Relevante**					
3	**Importante**					
4	**Crítico**					
5	**Vital**					

Fonte:SÊMOLA (2003 pag. 92).

Nesta etapa deve ser atingido o objetivo de classificar a sensibilidade dos principais ativos do colégio.

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

No que se diz respeito à gravidade, cabe a seguinte pergunta: *"Seria muito grave para o processo do negócio a quebra de segurança?"*. Aqui deve ser considerada a gravidade do impacto diretamente.

Na dimensão da urgência, a pergunta é a seguinte: *"Havendo a quebra de segurança, qual seria a urgência em solucionar os efeitos do ocorrido e em reduzir os riscos?"*. Aqui será considerado o tempo de duração do impacto associado diretamente.

Na dimensão tendência, a pergunta que cabe é: *"Qual seria a tendência dos riscos de segurança se nenhuma atividade preventiva ou corretiva fosse utilizada?"*. Aqui será considerada a variação da importância dos impactos associados diretamente.

A metodologia para a matriz GUT também aplica valores de 1 a 5 para indicar o grau de prioridade, conforme Tabela 6. Segundo 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. Como forma de facilitar a identificação dos processos e suas prioridades, o GUT Final é separado por faixas, e cada faixa receberá uma cor diferente:

- 1 a 42: **Verde**
- 43 a 83: **Amarela**
- 84 a 125: **Vermelha**

TABELA 7 – Escala para classificação de prioridades

Gravidade	Urgência	Tendência
1 – sem gravidade	1 – sem pressa	1 – não vai agravar
2 – baixa gravidade	2 – tolerante à espera	2 – vai agravar a longo prazo
3 – média gravidade	3 – o mais cedo possível	3 – vai agravar a médio prazo
4 – alta gravidade	4 – com alguma urgência	4 – vai agravar a curto prazo
5 – altíssima gravidade	5 – imediatamente	5 – vai agravar imediatamente

Fonte:SÊMOLA (2003 pag. 94).

Nesta etapa devem-se atingir os seguintes objetivos:

- mapeamento das prioridades dos principais ativos do colégio; e
- percepção das características de cada um dos ativos principais em função das dimensões GUT.

3.6 Matriz de Análise de Riscos

Conforme já foi mencionado no capítulo anterior, a construção de uma Matriz de Análise de Riscos é uma das ferramentas utilizadas na Análise de Riscos e Vulnerabilidades. Com a construção da matriz será possível organizar as prioridades, apoiar as decisões e implementar as medidas de segurança para cada perímetro da organização.

A NBR ISO/IEC 17799:2005 recomenda que em uma organização nas análises/avaliações de risco, os riscos sejam identificados, quantificados e priorizados, com base em critérios de aceitação e dos objetivos relevantes para a organização. E isso, pode ser obtido através da construção da Matriz de Análise de Riscos.

Entretanto os riscos de uma organização não estão somente associados ao número de falhas tecnológicas ou aos impactos potenciais. Diagnosticar o risco envolve o estudo de variáveis endógenas que vão além do aspecto tecnológico; sendo assim, devemos considerar também os aspectos humanos, aspectos físicos, legais e etc.

As técnicas de análise de risco podem ser aplicadas em toda organização, ou apenas em uma parte da mesma.

Fundamentalmente existem duas metodologias para orientar a análise de riscos, a **quantitativa** (voltada para mensurar os impactos financeiros em virtude de uma quebra de segurança) e **qualitativa** (orientada por medidas que proporcionam estimar os impactos provocados pela exploração de uma vulnerabilidade por uma ameaça).

Os métodos quantitativos baseiam-se no ROI - Retorno Sobre o Investimento, onde se estima a incidência de cada ameaça, baseando-se em históricos; estima-se o valor dos prejuízos que as ameaças podem causar; e estima-se o custo de combater essas ameaças. Ou seja, o investimento em controles de segurança deverá ser menor que a expectativa de perda anual com as ameaças levantadas

A metodologia qualitativa baseia-se em entrevistas para avaliar os níveis de risco prováveis de uma gama de ameaças e vulnerabilidades associadas. Baseados na experiência dos responsáveis pelos ativos, na inspeção física dos ambientes e na análise de documentação, atribuem-se notas à probabilidade de ocorrência do ataque e ao nível dos impactos.

Neste trabalho será utilizada a **metodologia qualitativa**.

Aspectos que devem ser considerados:

- relevância do processo/ativo;
- 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.

O estudo contempla ativos físicos e tecnológicos, assim a identificação de ameaças e vulnerabilidades será orientada com entrevistas com os gestores, observação, inspeções físicas presenciais aos ambientes e pesquisa nas documentações .

Tem-se observado como tendência, a realização de análise de risco e construção de matriz de analise de riscos, baseadas no levantamento dos controles de segurança (presença ou ausência), isto em virtude da credibilidade que a norma ISO/IEC 17799 obteve em relação a gestão de segurança da informação.

Por isso, alinham-se os resultados da matriz de análise de riscos aos controles da norma NBR ISO/IEC 17799:2005.

3.7 Conclusões Parciais

A NBR ISO/IEC 17799:2005 diz que certo número de controles pode ser considerado um bom ponto de partida para implementação de segurança da informação. Segundo a norma, deve-se começar construindo uma Política de Segurança da Informação. O próximo passo seria estabelecer os requisitos de segurança da informação, objetivo que pode ser atingido realizando a análise de riscos; e consultando legislações, regulamentos e normas vigentes. Após a análise de riscos, realizar a escolha dos controles e implementá-los.

A análise/avaliação de riscos da NBR ISO/IEC 17799:2005 deve identificar, quantificar e priorizar os riscos. Esses resultados devem orientar as ações de gestão apropriadas e as prioridades.

A metodologia apresentada objetiva cumprir de forma gradativa o que recomenda a NBR ISO/IEC 17799:2005 para implementação de seus controles. Assim, a metodologia propõe a construção da Política de Segurança, aplicar ferramentas como Mapeamento de Relevância, estudo de prioridades GUT e a construção de uma Matriz de Análise de Riscos onde com base nas ameaças, vulnerabilidades, probabilidade de ocorrência da ameaça e o impacto, pode-se analisar a implementação/escolha de um controle de segurança ou não.

4 IMPLEMENTAÇÃO DA NORMA

Este capítulo começa na sua primeira seção (4.1) com a descrição generalista de um colégio de forma geral, e com uma explanação sobre o colégio em estudo, o Colégio Militar de Santa Maria (CMSM).

Após a primeira seção, descreve-se o desenvolvimento de todas as atividades previstas no capítulo anterior (Procedimentos Metodológicos), a fim de implementar a norma NBR ISO/IEC 17799:2005 para os recursos de TI do CMSM.

A metodologia apresentada no Capítulo 3 desta dissertação, propõe a execução de cinco passos para se atingir os objetivos propostos por este trabalho:

- construir a Política de Segurança (seção 4.2);
- elencar os principais ativos (seção 4.3);
- construir o mapa de relevância dos ativos de TI (seção 4.4);
- montar a tabela de Impacto CIDAL e a Matriz GUT (seção 4.5); e
- obter a Matriz de Análise de Riscos do CMSM (seção 4.6).

No final deste capítulo faz-se a análise da implementação da norma (seção 4.7), onde se apresenta índices e os resultados obtidos, e por último as conclusões parciais (seção 4.8).

4.1 Estrutura de um Colégio

Segundo Kallas (2004), o organograma generalista de um colégio pode ser observado conforme a Figura 15, sendo as principais responsabilidades do diretor, secretaria e supervisão/orientação como seguem:

- **diretor -** elaborar e executar a proposta pedagógica da escola, administrar seu pessoal e seus recursos materiais, coordenar a administração financeira e contábil da escola, coordenar o processo de gestão estratégica, articular-se com as famílias e comunidade, criar processo de integração da sociedade com a escola, orientar o funcionamento da secretaria da escola, representar a escola junto aos demais órgãos, administrar o patrimônio da escola que compreende as instalações e outros;
- **secretaria -** organização do serviço de escrituração da escolar, executar as normas administrativas da escola, colaborar com a direção da unidade

escolar, no planejamento, execução e controle das atividades escolares; proceder a escrituração conforme disposto na legislação vigente, efetivar e registrar a matrícula, organizar as turmas preenchendo o diário de classe, relacionar nomes de alunos com documentos incompletos, preparar a pasta individual do aluno, preencher ficha individual, boletim ou caderneta escolar; levantar resultados do aluno e redigir a ata, preencher histórico escolar, atestados e declarações; atualizar o arquivo para atender as necessidades da escola; dentre outros;

- **supervisão/orientação -** coordenar o planejamento e implementação da proposta pedagógica da escola, coordenar a elaboração do currículo pleno da escola, envolvendo a comunidade escolar; assessorar os professores na escolha e utilização dos procedimentos e recursos didáticos mais adequados a atingir os objetivos curriculares, participar da elaboração do calendário escolar, articular os documentos de cada área para desenvolvimento do trabalho técnico-pedagógico da escola definindo suas atividades especificas, avaliar o trabalho pedagógico, sistematicamente, com vistas à reorientação de sua dinâmica; participar, com o corpo docente, do processo de avaliação externa e da análise de seus resultados; analisar os resultados da avaliação sistêmica feita juntamente com os professores e identificar as necessidades dos mesmos, analisar os resultados obtidos com as atividades de capacitação docente, na melhoria dos processos de ensino e de aprendizagem; identificar, junto com os professores as dificuldades de aprendizagem dos alunos; utilizar os resultados do levantamento como diretriz para as diversas atividades de planejamento do trabalho escolar;

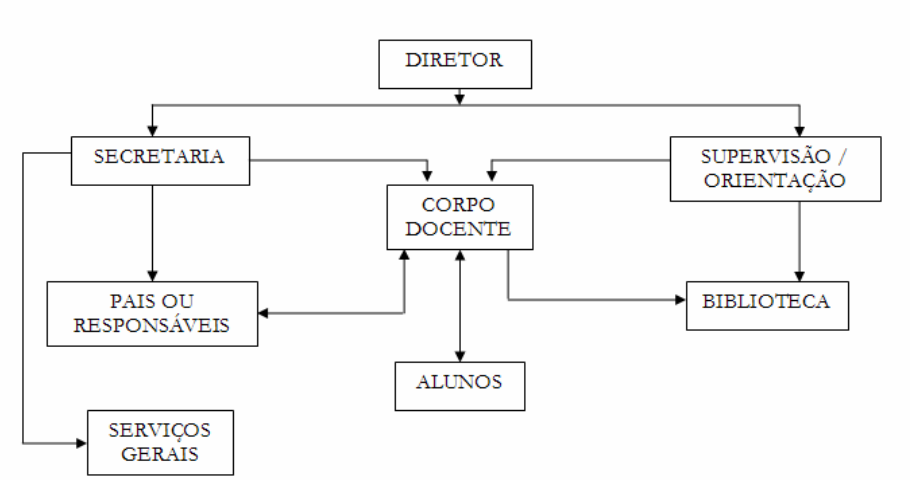


FIGURA 15 – Organograma genérico de uma escola

A estrutura organizacional de um colégio pode ser visualizada por três níveis (Figura 16): o Institucional (que compreende os órgãos de administração e gestão), o de Coordenação (conselhos de turmas, direções de turmas, conselho de docentes etc.) e o Técnico/operacional (salas de aula, professores e alunos).

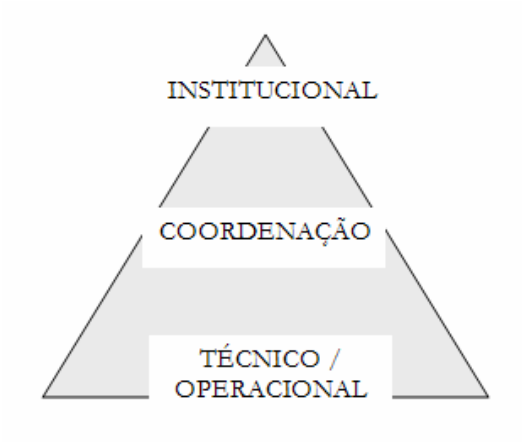


FIGURA 16 – Estrutura organizacional de um colégio

4.1.1 Colégio Militar de Santa Maria

A organização pedagógica do CMSM consiste em (Figura 17): Direção de Ensino (Cmdo), Divisão de Ensino, Seção Técnica de Ensino (STE), Seção Psicopedagógica, Seções de Ensino A (disciplinas de português, literatura e redação), B (matemática, desenho e informática), C (química, física e biologia), D (história, geografia e filosofia), E (educação

física), F (inglês e espanhol), Seção de Cursos, Seção de Meios Auxiliares e Seção de Expediente.

Essas seções têm as suas atribuições definidas no Regulamento dos Colégios Militares (R-69) e no Regimento Interno dos Colégios Militares. Devem trabalhar de maneira integrada entre si, com o Corpo de Alunos e a Divisão Administrativa.

O CMSM assim como os outros colégios militares do Brasil é hierarquizado como qualquer instituição militar, onde sempre é ressaltada a pessoa do Comandante e Diretor de Ensino, que será o responsável pela eficiência e pela eficácia da política educacional do Sistema de Ensino do Exército, buscando o desenvolvimento pleno dos seus objetivos, organizando e coordenando todos os esforços, oferecendo contínua inspiração e liderança em busca da permanente melhoria da qualidade do processo ensino-aprendizagem. Assim, além da parte de ensino, qualquer outra proposta ou política a ser aplicada e implementada no CMSM o apoio e a aceitação do Diretor de Ensino se faz imprescindível.

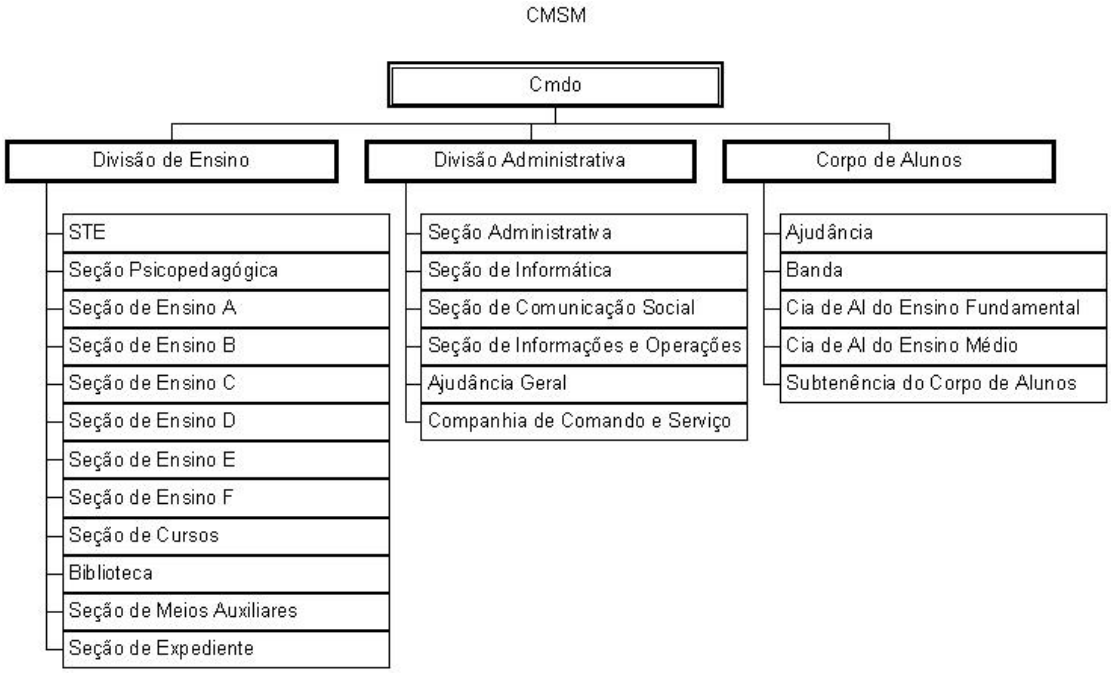


FIGURA 17 – Organograma do Colégio Militar de Santa Maria

Todas as seções do CMSM, mostradas na Figura 17, se encontram informatizadas e interligadas em rede. A rede de computadores do CMSM possui aproximadamente 140 microcomputadores conectados. Sendo que três destes computadores são servidores que oferecem serviços aos clientes (Figura 18).

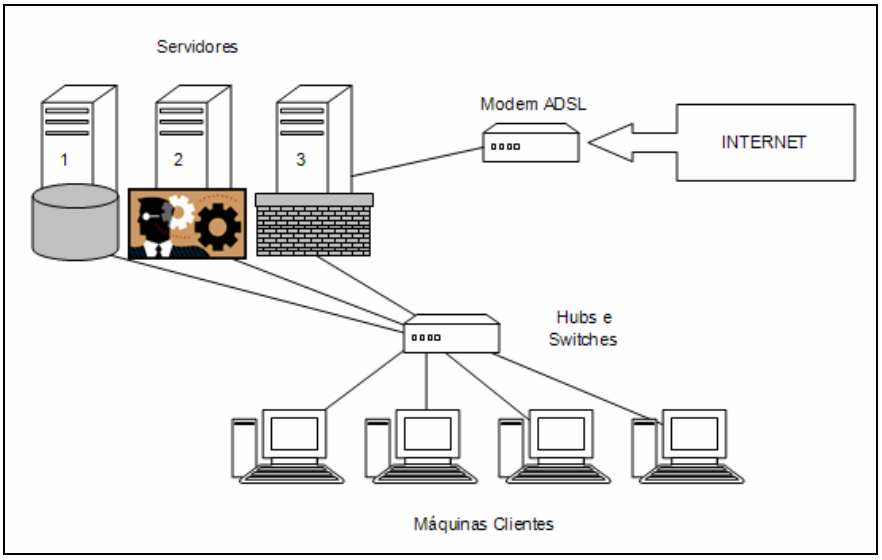


FIGURA 18 – Síntese da rede de computadores do CMSM

Com relação aos servidores, podemos sumariamente descrever as principais finalidades de cada um deles:

- **Servidor 1:** Servidor de Banco de Dados (armazena e mantém o banco de dados do principal sistema do CMSM o SGE[3]);
- **Servidor 2:** Servidor de Autenticação, Servidor de Aplicações Windows (SGE, SIMATEx[4], o sistema de ponto eletrônico) e servidor de armazenamento;
- **Servidor 3:** Servidor de página da Intranet do CMSM, mantém o PROTWEB[5], Firewall.

Para que se pudesse fazer um estudo sobre a Segurança da Informação em uma organização tipo colégio, mais precisamente no CMSM, conhecer como funciona o processo do negócio, saber quais são os setores envolvidos e quais são os recursos de TI disponíveis no

---

[3] Sistema de Gestão Escolar - programa de computador desenvolvido pelo Departamento de Ensino e Pesquisa (DEP) do Exército, o qual objetiva atender as necessidades da área de ensino e administrativo: necessidades de cadastramento de pessoal, controle de matrículas e graus, controle disciplinar, controle de biblioteca e saúde, controle de material e etc.

[4] Sistema de Controle de Material – programa desenvolvido pelo Centro de Desenvolvimento de Sistemas (CDS) do Exército, cuja finalidade é controlar o estoque de material bem como a quem pertence a carga do referido objeto.

[5] Protocolo Eletrônico – programa de computador destinado ao controle de circulação e despacho de documentação desenvolvido pelo CDS e especializado pela Seção de Informática do CMSM para uso interno.

tratamento das informações, se fazem de extrema necessidade. Assim, esta seção apresentou a estrutura generalista de um colégio e a estrutura organizacional do colégio em estudo (o CMSM).

Este trabalho de pesquisa foi realizado pelo *security officer* e integrante da Seção de Informática do CMSM. Colaborador este, que trabalha no colégio há mais de três anos na instituição, fator este que foi um grande facilitador para o correto levantamento das informações.

Esta etapa demandou sete dias de trabalhos, onde foram feitas verificações físicas dos setores e dos recursos de TI do CMSM, e consulta à documentações junto da Seção de Informática do CMSM.

Uma vez vencida esta etapa, partiu-se propriamente para o tratamento da Segurança da Informação no colégio.

4.2 Construção da Política de Segurança

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 no início dos trabalhos, obedecendo o que preconiza a NBR ISO/IEC 17799:2005, bem como as outras legislações do Exército Brasileiro (Portaria Nr. 483 do Exército, de 20 de setembro de 2001, que aprova as Instruções Gerais de Segurança da Informação para o Exército; e a Portaria Nr. 006 do Departamento de Ciência e Tecnologia do Exército - DCT, de 05 de fevereiro de 2007, que aprova as Normas para o Controle da Utilização dos Meios de TI no Exército) e a Lei Nº. 3505 – Política de Segurança da Informação para órgãos do Governo Federal.

O principal propósito da construção da Política de Segurança do CMSM foi o de informar aos usuários/colaboradores, professores e militares, as obrigações para a proteção da tecnologia e do acesso às informações digitalizadas. A política também objetivou oferecer um ponto referencial a partir do qual o *security officer* e a Seção de Informática pudessem configurar, adquirir e implementar mecanismos de segurança para atender os requisitos de segurança propostos.

Para política ser aceita, apropriada e efetiva, ela teve o suporte e a participação dos seguintes integrantes do CMSM na sua construção:

- diretor de ensino e comandante do CMSM;
- subdiretor de ensino e subcomandante;
- chefe da divisão administrativa do colégio;
- chefe da seção de informática; e
- integrantes técnicos em TI da seção de informática.

Além da participação, o diretor e o subdiretor do colégio sempre se mostraram favoráveis à criação e aplicação da política. Posturas estas demonstradas em diversas oportunidades, como em reuniões e formaturas, e de fundamental importância para a sustentabilidade da política e o correto acatamento das normas e procedimentos propostos por ela por parte de todo o colégio.

A política foi elaborada da forma que pudesse ser o mais viável a longo prazo e flexível possível. Assim, todos os seus termos procuraram ser aplicáveis independentemente de hardware e software específicos.

A Política de Segurança da Informação foi submetida para apreciação do diretor de ensino e comandante, sendo aprovada. Após, a mesma foi comunicada para toda a organização (usuários) de forma relevante, acessível e compreensível. A divulgação da política foi realizada da seguinte maneira:

- publicação na página da intranet do CMSM;
- publicação no Boletim Interno (BI – documento ostensivo e de publicação diária que dissemina as ordens do comando e direção de ensino do CMSM);
- explanação verbal pelo Chefe da Seção de Informática em duas oportunidades em reuniões formais com todos os colaboradores do CMSM; e
- afixação em murais do CMSM.

Muito do trabalho para a confecção da Política de Segurança para o colégio, refere-se à adequação da mesma à uma gama de legislações, portarias e normas que regem a organização Colégio Militar de Santa Maria. O trabalho demandou de reuniões com a direção e subdireção do colégio, além da equipe técnica em TI para aprovação da Política e trabalhos direcionados a todos os colaboradores com a finalidade de apresentá-la e divulgá-la.

Esta etapa demandou dez dias de atividades e estudos. A Política de Segurança pode ser visualizada no Apêndice A desta dissertação.

4.3 Principais Ativos

Segundo o Capítulo 7 “Gestão de Ativos” da NBR ISO/IEC 17799:2005 no seu item 7.1.1 “Inventário dos Ativos”, se faz de suma importância que todos os ativos devam ser claramente identificados e inventariados. Entretanto, neste estudo de caso os ativos em questão ficaram restritos aos recursos de tecnologia de informação. Pois nosso trabalho se propõe a proporcionar uma melhor segurança da informação para os recursos e informações que dependem da tecnologia da informação.

Os ativos são essenciais para as atividades que compõem a solução. A identificação dos principais ativos foi obtida em reuniões específicas com os principais gestores e representantes de cada um dos setores do colégio. A finalidade de reunir um representante de cada setor foi o de obter a correta relação entre as atividades desenvolvidas por cada um desses setores ao ativo de TI necessário para a realização do processo.

Além das reuniões, foi realizada uma atividade investigativa e de entrevistas em loco com os funcionários e gestores de diferentes setores do Colégio. Assim, foram levantados os ativos listados na Tabela 07. Como resultado, a Tabela 07 apresenta os principais recursos de TI do Colégio, ativos estes que proporcionam as informações e recursos necessários para o andamento das atividades e manutenção dos processos do negócio da organização.

O Servidor 1, é um computador tipo servidor onde fica instalado e configurado o banco de dados principal do colégio, é um banco de dados tipo *PostgreSQL* que mantém armazenado toda a vida acadêmica dos alunos do CMSM (históricos, boletins, comportamento), dados pessoais e profissionais dos colaboradores do colégio, estoque do almoxarifado. Informações estas vitais para a organização.

O Servidor 2, é um computador tipo servidor onde se encontra armazenado o SGE (sistema de interface com o banco de dados do Servidor 1 utilizado pelos usuários) que é o software de maior utilização e importância para o negócio do colégio, pois é através dele que são consultadas e inseridas as informações principais para o colégio no banco de dados do Servidor 1. Neste computador também se encontra instalado o SIMATEx, sistema que controla o material físico do CMSM (valor patrimonial, seção e responsável pelo material, local em que se contra alocado, etc.) e o sistema de ponto eletrônico, programa destinado a controlar os horários de trabalho dos colaboradores do CMSM.

TABELA 08 – Principais ativos dos recursos de TI do Colégio

ATIVO	OBSERVAÇÃO
Servidor 1	Servidor de Banco de Dados (armazena e mantém o banco de dados do principal sistema do CMSM o SGE).
Servidor 2	Servidor de Autenticação, Servidor de Aplicações Windows (SGE, SIMATEx, sistema de ponto eletrônico) e servidor de armazenamento.
Servidor 3	Servidor de página da Intranet, armazena o PROTWEB, Firewall.
Rede de Computadores	Todos os serviços disponibilizados pelo sistema de rede como um todo, não particionado por cabeamento, estações de trabalho, internet / intranet e etc.
Internet	Sistema que proporciona a disponibilização de acesso a Internet aos computadores do Colégio.
Intranet	Destinada a parte de comunicação, divulgação de noticias e procedimentos.
Firewall	Controla a troca de dados digitais da Rede do Colégio com a Internet.
Estações de Trabalho	Computadores tipo PC ou clientes da rede do colégio, para uso exclusivo para rotinas de trabalho dispostos nas diversas seções para os professores, militares e funcionários civis do CMSM.
Banco de Dados	Banco de Dados do SGE
SGE	Sistema de Gestão Escolar - programa de computador desenvolvido pelo DEP, o qual objetiva atender as necessidades da área de ensino e administrativo, o qual responde as necessidades de cadastramento de pessoal, controle de matrículas e graus, controle disciplinar, controle de biblioteca e saúde, controle de material e etc.
SIMATEx	Sistema de Controle de Material – programa desenvolvido pelo Centro de Desenvolvimento de Sistemas do Exército (CDS), cuja finalidade é controlar o estoque de material bem como a quem pertence a carga do referido objeto.
PROTWEB	Protocolo Eletrônico – programa de computador destinado ao controle de circulação e despacho de documentação desenvolvido pelo CDS e especializado pela Seção de Informática do CMSM para uso interno.
Informações Armazenadas no Servidor de armazenamento	Documentos e informações digitalizadas, sigilosas ou não, armazenadas no servidor.
Cabeamento	Toda a infra-estrutura física para inter-conectividade dos computadores que pertencem ao CMSM.
Sistema de Câmeras	Programa de computador e equipamentos destinados a prover o sistema de vigilância por câmeras.

O Servidor 3, é um computador tipo servidor que mantém o *firewall* da rede, que possui as regras de acesso à Internet. Encontra-se também neste servidor a página da Intranet do colégio, importante fonte de difusão de informações e comunicados a todos os integrantes. O sistema de protocolo eletrônico (PROTWEB) da mesma forma é mantido por esta maquina,

este é um software importante para a agilização da circulação e despacho de documentação interna do colégio.

A Rede de Computadores é um ativo de fundamental importância, pois a mesma além de proporcionar o compartilhamento de recursos, é através dela que as maquinas clientes utilizadas pelos professores e funcionários do colégio acessam os sistemas coorporativos, a Internet e a Intranet.

A Internet é um recurso importante para pesquisa por parte dos professores e alunos. Em igual importância ela é utilizada pela Divisão Administrativa do colégio para envio de arquivos a outros órgãos a que o colégio se subordina, e acesso a documentação externa.

A Intranet cumpre a principal finalidade a que se destina, que é o de informar e difundir informações do colégio e que se destinam de forma ostensiva a todos os públicos.

Firewall, importante sistema de controle de utilização da Internet por parte dos usuários da rede do colégio, e como barreira principal contra invasões e acessos indevidos.

As estações de trabalho são as principais ferramentas tecnológicas utilizadas pelos usuários do colégio, é onde eles acessam os programas coorporativos do CMSM, acessam a Intranet, acessam a Internet, arquivam localmente arquivos de trabalho e acessam arquivos armazenados nos servidores.

Banco de Dados principal, software mantido pelo Servidor 1 da rede do CMSM, onde estão localizadas informações vitais dos alunos e colaboradores do colégio.

Sistema de Gestão Escolar (SGE), software armazenado no Servidor 2 do CMSM, com a finalidade de realizar a interface do usuário com o banco de dados do Servidor 1, e responsável por disponibilizar ao usuário as informações que ele necessita.

Sistema de Controle de Material do Exército (SIMATEx), sistema mantido pelo Servidor 3, e que faz o controle patrimonial dos materiais do colégio. Muito importante particularmente para a Divisão Administrativa do colégio.

O PROTWEB, é um sistema desenvolvido com a finalidade de agilizar o despacho de documentação interna do colégio pela rede de computadores, sem a necessidade da circulação de papel.

Muitas informações e arquivos de usuários, que não fazem parte do banco de dados de dados principal, encontram-se armazenadas no Servidor 2, muitas vezes arquivos importantes ou de caráter sigiloso, por isso é necessário ter-se os devidos cuidados de segurança com estas informações.

O cabeamento é um ativo físico que proporciona o correto funcionamento da rede de computadores do colégio militar.

O sistema de câmeras do colégio é composto por um computador tipo PC (*personal computer*) que capta imagens de 06 micro-câmeras distribuídas pelos corredores do colégio, destinado ao controle do fluxo dos alunos e das entradas e saídas das salas de aula.

O levantamento de todos os ativos de TI relevantes no CMSM, listados na Tabela 07, 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. Também foi necessário disponibilidade de tempo dos gestores para entrevistas e reuniões.

4.4 Relevância

Após ter passado por todos os setores do Colégio, ter conhecido mais profundamente o funcionamento do negócio e ter conversado com os principais gestores dos ativos, foi feito o mapeamento da relevância de cada um deles.

TABELA 09 – Classificação da Relevância

ATIVO	RELEVÂNCIA
Banco de Dados	**5**
SGE	**5**
Servidor 1	**4**
Servidor 2	**4**
Informações Armazenadas no Servidor de armazenamento	**4**
Rede de Computadores	**3**
SIMATEx	**3**
Cabeamento	**3**
Sistema de Câmeras	**3**
Firewall	**3**
Servidor 3	**2**
Internet	**2**
Estações de Trabalho	**2**
PROTWEB	**2**
Intranet	**1**

ESCALA	
1	Não Considerável
2	Relevante
3	Importante
4	Crítico
5	Vital

Esta atividade visa evitar discrepâncias na priorização das atividades que comporão a solução.

Como podem ser visualizados na Tabela 08 (Classificação da Relevância) os ativos de TI do CMSM foram dispostos em ordem de importância para o negócio da organização. Podemos destacar o Banco de Dados, o sistema SGE, o Servidor 1 e o Servidor 2.

Para realização deste trabalho foi necessária uma reunião com os principais gestores dos ativos envolvidos e representantes dos diferentes setores do colégio. A reunião baseou-se na discussão da importância de cada um dos ativos para os processos do negócio (rotinas de trabalho).

Esta etapa demandou aproximadamente quatro dias.

4.5 Impactos CIDAL e Prioridades GUT

Após a realização das duas etapas anteriores, foi realizado um estudo para levantar a sensibilidade de cada um dos ativos para o caso da ocorrência da quebra de segurança. Esta etapa também visa fornecer uma gama de propriedades que identificam a necessidade de priorização de quais os ativos necessitam de resposta com mais urgência.

Foram realizadas entrevistas individuais com os gestores de cada ativo e os representantes de cada setor do colégio. Os mesmos critérios de escala utilizados para o levantamento da Relevância foram utilizados aqui, tanto para construção da tabela que fornece os dados do Impacto CIDAL como da Matriz GUT.

Foram feitas reuniões com a equipe de TI do colégio para montagem da Tabela 09 (Matriz GUT) e Tabela 10 (Impacto CIDAL).

Pode-se observar que tanto na Tabela 09 (Matriz GUT) como na Tabela 10 (Impacto CIDAL) que alguns ativos se destacam, como: Servidor 1, Servidor 2, Banco de Dados e SGE. São os mesmos ativos que já haviam se destacado no mapeamento da relevância no passo metodológico anterior.

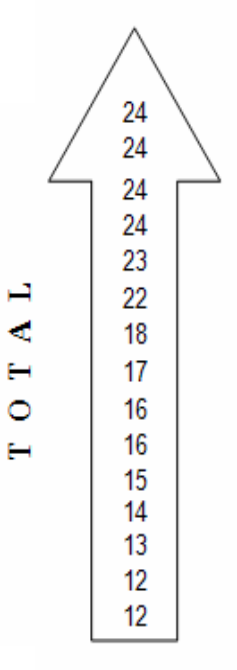
TABELA 10 – Matriz GUT

PROCESSO / ATIVO	GRAVIDADE	URGÊNCIA	TENDÊNCIA	Total (GxUxT)
Servidor 1	5	5	4	100
Servidor 2	5	5	4	100
Banco de Dados	5	5	4	100
SGE	5	5	4	100
Informações Armazenadas no Servidor de armazenamento	4	3	4	48
Rede de Computadores	3	3	4	36
Firewall	3	3	4	36
Cabeamento	3	3	4	36
SIMATEx	3	2	3	18
Internet	2	2	3	12
Sistema de Câmeras	2	2	3	12
Servidor 3	2	1	3	6
Estações de Trabalho	3	1	2	6
Intranet	2	1	2	4
PROTWEB	2	1	2	4

Gravidade	Urgência	Tendência
1 – sem gravidade	1 – sem pressa	1 – não vai agravar
2 – baixa gravidade	2 – tolerante à espera	2 – vai agravar a longo prazo
3 – média gravidade	3 – o mais cedo possível	3 – vai agravar a médio prazo
4 – alta gravidade	4 – com alguma urgência	4 – vai agravar a curto prazo
5 – altíssima gravidade	5 - imediatamente	5 – vai agravar imediatamente

TABELA 11 – Impacto CIDAL

ATIVO	CONCEITOS			ASPECTOS		TOTAL
	CONFIDEN-CIALIDADE	INTEGRI-DADE	DISPONIBI-LIDADE	AUTENTI-CIDADE	LEGALI-DADE	
Servidor 1	5	5	5	5	4	24
Servidor 2	5	5	5	5	4	24
Banco de Dados	5	5	5	5	4	24
SGE	5	5	5	5	4	24
Firewall	5	5	4	5	4	23
Informações armaz.	5	5	3	5	4	22
SIMATEx	2	4	4	4	4	18
Rede de Computadores	4	4	4	3	2	17
Servidor 3	3	4	4	3	2	16
Estações de Trabalho	4	4	3	2	3	16
Cabeamento	3	4	4	2	2	15
PROTWEB	3	3	2	4	2	14
Intranet	2	4	3	2	2	13
Internet	3	3	2	2	2	12
Sistema de Câmeras	3	2	2	3	2	12



ESCALA	
1	Não Considerável
2	Relevante
3	Importante
4	Crítico
5	Vital

Este trabalho foi oneroso no sentido de que os envolvidos nas entrevistas individuais (gestores dos ativos e representantes dos diversos setores) e a equipe técnica de TI do Colégio, precisavam passar por um nivelamento de conhecimento de Segurança da Informação, principalmente nos conceitos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade. E também para correta compreensão do dimensionamento dos conceitos de gravidade, urgência e tendência. Assim antes do início dos trabalhos foi necessária uma palestra a estes participantes onde foram apresentados os conceitos anteriormente citados.

Para realização desta etapa foram necessárias além das entrevistas com os principais gestores e representantes dos setores do colégio, mais duas reuniões com a equipe especialista em TI do colégio. Etapa que demandou aproximadamente sete dias, muito devido a necessidade de preparação de material e nivelamento de conhecimentos por parte dos envolvidos.

4.6 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.

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 e representantes dos setores do colégio, através de observação, inspeções físicas presenciais aos ambientes, e pesquisa a documentações.

A matriz construída 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.

Considerando a lista de ativos que já havia sido levantadas em etapas anteriores (seção 4.3), a confecção da matriz envolveu:

- pesquisas das principais ameaças atualmente a nível de tecnologia da informação;

- estudos, pesquisas a bibliografias específicas, consultas a Internet e revistas de segurança, no sentido de levantar quais eram as maiores vulnerabilidades de cada ativo;
- pesquisas para obtenção de estatísticas de ataques das principais ameaças levantadas;
- mensuração do impacto para a organização no caso da ameaça explorar a vulnerabilidade e causar um incidente de segurança; e
- indicação de medidas de segurança para redução do risco.

As medidas de segurança apontadas pela matriz de análise de riscos foram alinhadas aos controles da norma NBR ISO/IEC 17999:2005, conforme se pode observar no Apêndice A desta dissertação.

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 necessários vinte e um dias de estudos, pesquisas e anotações.

4.7 Análise da Implementação da Norma

Quando da decisão para o início desta pesquisa e realização do trabalho, foi necessária a aquisição de conhecimento sobre o estado da arte da Segurança da Informação no cenário atual. Através de revisões de literatura, discussões com a equipe técnica em TI do colégio, pesquisas a trabalhos científicos e dissertações em instituições de ensino superior, chegou-se a um consenso de que a NBR ISO/IEC 17799:2005 seria o documento mais indicado e completo atualmente para uma correta gestão de Segurança da Informação.

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, ter uma variabilidade significativa, podendo requerer uma consultoria. No caso do colégio, não foi usado consultoria externa, pois se assume que esta tarefa pode ser realizada pelo *security officer*.

Deve-se ter a noção de que nem todos os controles recomendados pela norma são necessários de serem implementados. Isto otimiza o processo de implementação da norma.

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 envolver diretamente a direção, e dispor de uma metodologia consciente, capaz de orientar os trabalhos e transformar as atividades em redução nos riscos.

A norma NBR ISO/IEC 17799:2005 tem o nítido papel de apontar os principais aspectos que se deve dar atenção, ou seja, a mesma orienta O QUE se deve fazer e não COMO fazer, assim, não dispõe uma metodologia para realização das atividades. Então, se fez necessário aplicar ferramentas metodológicas condizentes e capazes de guiar os trabalhos e transformar os resultados reais em redução dos riscos.

Existem metodologias propostas de diferentes formas, porém deve-se escolher a que melhor se alinha com a norma que se pretende adotar.

O capítulo 3, apresenta a metodologia empregada neste trabalho para a implementação da norma NBR ISO/IEC 17799:2005. As ferramentas metodológicas foram:

- confecção da Política de Segurança;
- planilha de identificação de ativos físicos e tecnológicos;
- mapa de relevância; e
- estudos dos impactos CIDAL e prioridades GUT.

Estas ferramentas ajudaram na:

- construção da Matriz de Análise de Riscos.

Observou-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, políticas de segurança e confecção de documentação. Todos estes requisitos foram tratados por ocasião da aplicação da metodologia proposta para realização deste trabalho.

É ponto pacífico de que não se é possível 100% de segurança, mesmo implementando todos os controles propostos pela norma NBR ISO/IEC 17799.

4.7.1 Pontos mais Relevantes para Implementação

Para a realização desta pesquisa as principais atividades desenvolvidas foram: realização de uma revisão de literatura, estudo da NBR ISO/IEC 17799:2005, estudo sobre a estrutura do colégio, construção da Política de Segurança, levantamento dos ativos de TI envolvidos nas atividades e processo do negócio, realização do mapeamento de relevância, construção da Tabela de Impacto CIDAL e da Matriz GUT, e a confecção da Matriz de Análise de Riscos alinhada com a norma NBR ISO/IEC 17799:2005.

Da revisão de literatura, tendo como referencial teórico ou prático o uso da NBR ISO/IEC 17799, foi constatado que, pelo nosso conhecimento, inexistem trabalhos com foco em colégios.

Para conhecimento da norma, foi feita uma leitura crítica da norma NBR ISO/IEC 17799 versões do ano de 2001 e a mais atual do ano de 2005 pelo *security officer* do colégio e discutido com a equipe de TI do colégio os principais controles. Também foram analisadas outras pesquisas e dissertações a respeito da referida norma. Trabalho este que foi permeado durante todo o andamento desta dissertação.

A atividade de apresentar a estrutura genérica de um colégio e as peculiaridades do colégio do estudo de caso, foi realizada pelo *security officer* e integrante da Seção de Informática do CMSM. Por ser realizada por um colaborador da própria organização e com perfil tecnológico, tornou o trabalho mais fácil e ágil. A atividade levou sete dias para ser concluída, com base em verificações físicas dos setores e dos recursos de TI do CMSM, e consulta a documentações junto da Seção de Informática do CMSM.

Os principais pontos a serem destacados quando da confecção da Política de Segurança são:

- foi necessário a leitura de uma gama de legislações, portarias e normas que regem a organização Colégio Militar de Santa Maria para não ir de encontro a um destes documentos;
- foram necessárias reuniões com a direção e subdireção do colégio, além da equipe técnica em TI para aprovação da Política;
- foi conseguido apoio e sustentação necessários junto a alta direção do colégio para a aplicação da Política de Segurança; e

- foi necessário um trabalho de divulgação e disponibilização do documento da Política de Segurança da Informação, para que fosse de conhecimento e aceitação por parte de todos os integrantes do colégio.

Assim a Política de Segurança é o ponto inicial de qualquer organização que deseja iniciar um processo de gestão de segurança da informação, pois através do processo de confecção da política foi obtido o apoio da alta direção do colégio, através da sua divulgação foi feito um trabalho junto aos colaboradores para ressaltar a importância da segurança da informação, além de que a política serviu como um referencial junto com a Matriz de Análise de Riscos para a adoção de controles de segurança.

O levantamento e descrição dos principais ativos do colégio foram realizados pelo Chefe da Seção de Informática, o *security officer* do Colégio, e levou cinco dias de trabalho.

Para se realizar o Mapeamento da Relevância, foi importante reunir-se com os principais gestores dos ativos e representantes de cada setor do colégio, para que se pudesse ser feito o mapeamento da relevância de cada um deles. Esta foi a etapa que menos demandou tempo para sua realização (quatro dias), pois a tabela proposta a se construir não é de muita complexidade e com apenas uma reunião com os principais gestores dos ativos e representantes de cada setor do colégio, foi possível fazer as anotações pertinentes e a posteriori construir o mapa de relevância dos ativos.

O trabalho de construção da Tabela de Impacto CIDAL e da Matriz GUT foi oneroso no sentido de que os envolvidos nas entrevistas individuais (gestores dos ativos) e os especialistas da área de TI, precisaram passar por um nivelamento de conhecimento, principalmente nos conceitos do que é Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade; e para compreenderem o real dimensionamento para Gravidade, Urgência e Tendência, para a correta montagem da Matriz GUT. Para realização desta etapa realizaram-se duas reuniões com os principais gestores dos ativos e mais duas reuniões com a equipe especialista em TI do colégio, o que demandou aproximadamente sete dias, devido a necessidade de preparação de material e nivelamento de conhecimentos.

Porém, a Matriz de Análise de Riscos tende a ser o ponto mais importante e oneroso do processo de implantação. As implementações dos controles de segurança são feitos com base nos dados levantados pela matriz e no que recomenda a NBR ISO/IEC 17799:2005, daí advém sua importância. Foi a etapa que mais demandou esforços para realização, seja no fator estudo e pesquisa, seja no fator tempo. Pois, requereu um estudo específico de cada ativo, porque cada ativo possui particularidades próprias e muito especializadas no sentido de:

- estudar as ameaças que cada um está sujeito;
- levantar as vulnerabilidades que cada um possui;
- descobrir a probabilidade da ocorrência da ameaça;
- mensurar o impacto no caso do incidente de segurança; e
- associar uma medida de segurança cabível e em conformidade com a norma NBR ISO/IEC 17799:2005.

Além das atividades citadas anteriormente, outros aspectos também foram levados em consideração por ocasião da confecção da matriz, aumentado a complexidade da etapa. Aspectos como: relevância do ativo, projeção do impacto, posição do ativo na tabela de Impacto CIDAL e da Matriz GUT.

A norma NBR ISO/IEC 17799:2005 trata de alguns fatores críticos de sucesso tais como: a existência de uma Política de Segurança alinhada com os objetivos do negócio, o comprometimento dos mais altos níveis gerencias à Política de Segurança, provisão de recursos financeiros, e trabalho de conscientização da importância da Segurança da Informação. Esses fatores devem e foram considerados na gestão da segurança da informação do colégio em estudo.

A existência de uma Política de Segurança alinhada com o negócio da organização deixou de ser pendência quando da sua confecção em conformidade com a NBR ISO/IEC 17799:2005 e as legislações que regem o colégio.

Quando da aprovação e divulgação, foram destacados o apoio e sustentabilidade da direção e subdireção do colégio à Política de Segurança. Por ocasião da divulgação da Política de Segurança, foi trabalhado pelo *security officer* em duas palestras proferidas aos colaboradores do colégio a importância da Segurança da Informação, trabalhando a conscientização para o assunto.

Quanto a provisão de recursos financeiros, os mesmos foram disponibilizados de acordo com as possibilidades do orçamento do colégio, e tratado em mais detalhe na seção que se segue.

Assim, pode-se dizer que também foi importante para o sucesso do trabalho a observância dos fatores críticos de sucesso recomendados pela norma.

4.7.2 Discussão sobre Custos de Implementação

Conforme o tamanho e a complexidade da organização em que se propõe a estabelecer uma Gestão da Segurança da Informação, se faz necessário um estudo de custo e benefício antes de se assumir sozinho a implementação de um sistema de Gestão da Segurança da Informação, podendo ser necessária consultoria externa.

O trabalho proposto visa proteger os recursos de TI do CMSM que mantém os processos do negócio e as informações vitais, usando como guia a NBR ISO/IEC 17799:2005. O colégio possui uma Seção de Informática composta por quatro profissionais, onde três profissionais possuem grau superior em áreas tecnológicas e o quarto componente possui curso técnico em informática. Assim, num primeiro momento não se fez necessário o apoio de consultoria externa. Portanto, não houve gastos com consultoria externa, apenas horas de trabalho da própria equipe.

Para iniciar o trabalho, a aquisição da norma NBR ISO/IEC 17799:2005 se fez necessária. O custo da norma, segundo o site da ABNT (http://www.abnt.org.br), é atualmente R$ 153,80 (Cento e cinqüenta e três reais e oitenta centavos), seja a mesma impressa ou eletrônica para impressão sob demanda.

Além da norma, foi necessário a aquisição de documentação sobre Segurança da Informação e livros técnicos, para consulta e estudo do pessoal envolvido em Segurança da Informação, particularmente o *security officer*. Assim, foram adquiridos dois livros sobre Segurança da Informação:

- Gestão da Segurança da Informação: Uma visão executiva, do autor Marcos Sêmola, editado pela Editora Campus em 2003. R$ 55,00 (cinqüenta e cinco reais); e
- Linux: Servidores de Rede, do autor Craig Hunt, lançado pela editora Ciência Moderna LTDA, Rio de Janeiro, 2004. R$ 120,00 (cento e vinte reais).

Também foram necessárias modificações de ordem física nas dependências da organização como:

- colocação de placas “Acesso Restrito” em algumas portas;
- reestruturação de algumas partes do cabeamento de rede de computadores; e
- confecção de claviculários para controle de chaves.

A necessidade de treinamento é sempre um fator preponderante a ser considerado. Assim foi constatada a necessidade de atualização técnica por parte do responsável da Segurança da Informação em recursos de TI. Portanto, foi realizado pelo referido profissional um curso de administração e segurança em computadores com sistema operacional Linux, em virtude da mudança do padrão de sistemas operacionais adotado pelos computadores tipo servidores do colégio. O curso custou R$ 2.052,00 (dois mil e cinqüenta e dois reais) e foi realizado em empresa de tecnologia sediada nesta cidade.

No tocante ao tempo gasto para realização do trabalho, pode-se observar a Figura 19 e 20, o número de dias necessários para o cumprimento das etapas que haviam sido propostas.

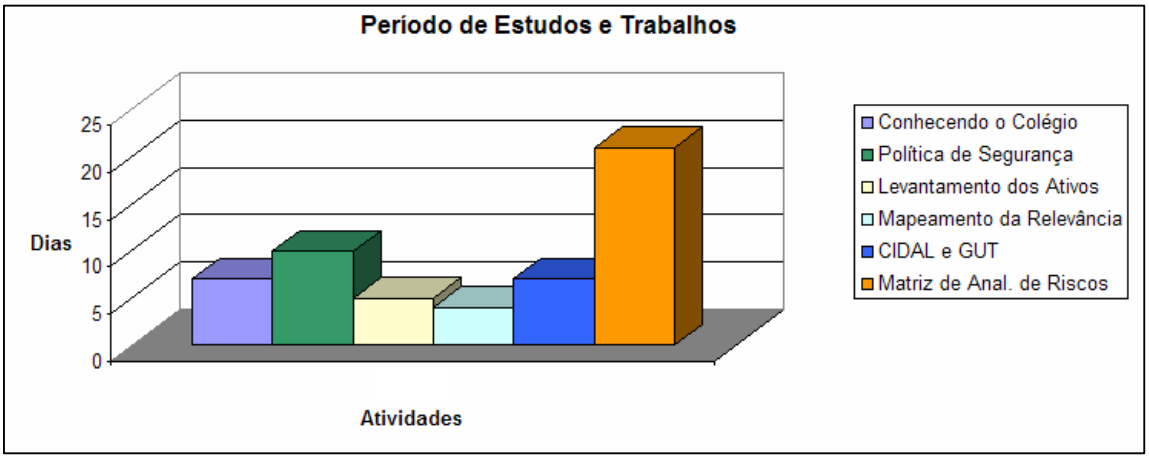


FIGURA 19 – Tempo em dias dos trabalhos realizados

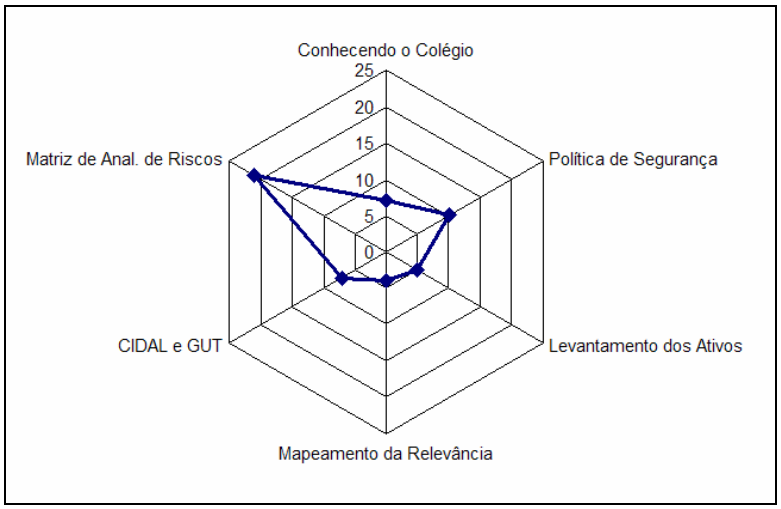


Figura 20 – Tempo em dias

Constata-se pelas Figuras 19 e 20, que das etapas metodológicas a se cumprirem as que mais necessitaram de tempo para execução foram a construção da Matriz de Análise de Riscos (vinte e um dias) e a confecção da Política de Segurança (dez dias).

No que diz respeito ao custo no tocante a recursos humanos, consideramos o dia trabalhado com oito horas, a semana com cinco dias úteis, e o mês com quatro semanas. E para fins didáticos consideramos, rendimentos estimados por mês do diretor e subdiretor do colégio como sendo R$ 4.000,00 (quatro mil reais), dos gestores e do *security officer* R$ 3.000,00 (três mil reais), da equipe de TI R$ 2.000,00 (dois mil reais) e dos representantes dos diversos setores do colégio R$ 1.000,00 (mil reais).

Assim, calculando-se obtivemos o valor do custo por hora do diretor e subdiretor de R$ 25,00/h, dos gestores e do *security officer* de R$ 18,75/h, da equipe de TI de R$ 12,50/h e representantes dos diversos setores do colégio de R$ 6,25/h.

A Tabela 11 retrata o custo do pessoal envolvido em cada etapa da realização deste trabalho. O custo demonstrado nesta tabela é considerado por colaborador, ou seja, a exceção do *security officer*, do diretor e do subdiretor, que são representados por somente uma pessoa. O grupo dos gestores e a equipe de TI são formados por mais de um colaborador cada.

TABELA 12 – Síntese de custos em recursos humanos

ETAPA	RECURSOS HUMANOS	ENVOLVIMENTO EM HORAS	CUSTO (R$)
Estudo do Colégio	- Security Officer	7 dias = 56 horas	1.050,00
Construção da Política de Segurança	- Security Officer - Equipe de TI - Diretor do colégio - Subdiretor do colégio	10 dias = 80 horas 4 dias = 32 horas 2 dias = 16 horas 2 dias = 16 horas	1.500,00 400,00 400,00 400,00
Levantamento de Ativos	- Security Officer - Gestor - Representantes do setores	5 dias = 40 horas 1 dia = 8 horas 1 dia = 8 horas	750,00 150,00 50,00
Mapeamento da Relevância	- Security Officer - Gestor - Representantes do setores	4 dias = 32horas 1 dia = 8 horas 1 dia = 8 horas	600,00 150,00 50,00
CIDAL e GUT	- Security Officer - Equipe de TI - Gestor - Representantes do setores	7 dias = 56 horas 4 dias = 32 horas 2 dias = 16 horas 2 dias = 16 horas	1.050,00 400,00 300,00 100,00
Matriz de Análise de Riscos	- Security Officer - Equipe de TI	21 dias = 168 horas 21 dias = 168 horas	3.150,00 2.100,00

Os gráficos apresentados nas Figuras 21 e 22, resumem a Tabela 11, ou seja, demonstram o custo total das horas trabalhas por tipo de colaborador envolvido no cumprimento das etapas propostas.

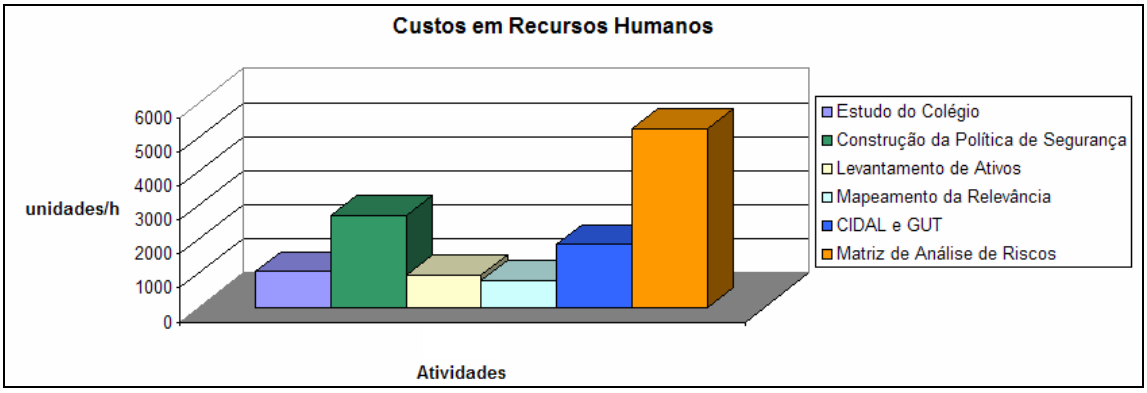


Figura 21 – Custo total em recursos humanos

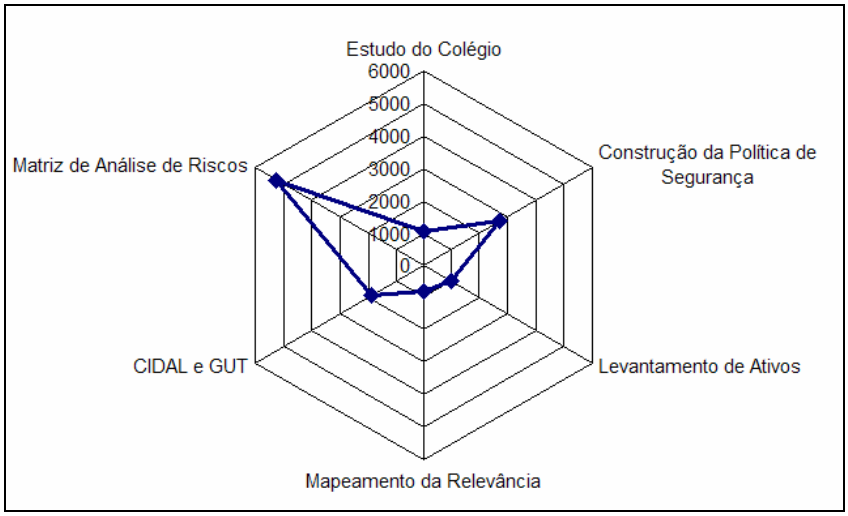


Figura 22 – Custo total de horas trabalhadas

Podemos concluir com base nos gráficos apresentados, que a relação entre o tempo necessário para o cumprimento de cada etapa com o custo da hora trabalhada está intimamente correlata. Pois, as etapas que mais levaram tempo para serem concluídas, também foram as que obtiveram o maior custo da hora trabalhada.

A Tabela 12, retrata o total gasto por cada recurso humano para o cumprimento do trabalho proposto. Estes custos foram obtidos através do somatório dos custos de cada profissional e que foi retratado na Tabela 11.

É importante ressaltar que, no caso do colégio em estudo e aplicação da metodologia proposta, o número de profissionais que compõem a equipe de TI são três (02 com curso superior em tecnologia e 01 técnico em informática, todos da Seção de Informática do CMSM), e o número de representantes dos diferentes setores do colégio e também

participaram de atividades como reuniões e entrevistas foram de oito pessoas: dois integrantes do Corpo de Alunos, dois integrantes da Divisão de Ensino, três integrantes da Divisão Administrativa, e um integrante do corpo docente.

TABELA 13 – Custo total por colaborador

PROFISSIONAL ENVOLVIDO	CUSTO TOTAL (R$)
Diretor do Colégio	**400,00**
Subdiretor do Colégio	**400,00**
Security Officer	**8.100,00**
Gestor	**600,00**
Equipe de TI	**8.700,00**
Representantes dos setores do Colégio	**1.600,00**

Conforme pode ser visualizado na Figura 23, gráfico que retrata a Tabela 12, os dois tipos de profissionais que mais se envolveram e tiveram custos de hora trabalhada foram o *security officer* e a equipe de TI. Seguindo com terceiro maior custo de hora trabalhada os representantes de cada setor chave do colégio.

Figura 23 – Custo total por profissional envolvido

O maior custo envolvido foi o da equipe de TI, pois depois do *security officer*, foi o tipo de profissional que mais se envolveu em atividades. Porém, seu custo também foi influenciado pela quantidade de profissionais envolvidos na equipe, para a complexidade e nível de informatização no colégio do estudo de caso a equipe de TI com três integrantes se mostrou suficiente, número de integrantes que pode variar conforme as especificidades da organização em que se vai aplicar a metodologia de trabalho.

O segundo maior custo envolvido, foi o do *security officer*, isto se deve ao fato do mesmo ser peça fundamental para a Gestão da Segurança da Informação. Este profissional além de ser o responsável por todo o projeto de segurança, também foi o que mais absorveu horas de trabalho e participou de todas as atividades.

Os dois custos mais baixos foram os dos profissionais de nível gerencial e de comando da organização (diretor e subdiretor de ensino do colégio), isto devido a participação dos mesmos ter sido mais efetiva no início dos trabalhos por ocasião da confecção da Política de Segurança do CMSM. Apesar de estes colaboradores terem a menor participação em horas envolvidas, menor custo de horas necessárias, participado das reuniões somente da confecção da Política, seu envolvimento não deixa de ser menos importante, pois, sem o apoio e aprovação das pessoas de nível estratégico da organização a realização do trabalho não seria efetivada.

4.8 Conclusões Parciais

Ter conhecimentos sobre os principais aspectos e conceitos importantes sobre Segurança da Informação é o passo inicial para qualquer profissional que vai iniciar um projeto de segurança. Uma vez escolhida uma norma ou uma metodologia, estudá-las e compreendê-las deve ser o próximo passo, assim o estudo da NBR ISO/IEC 17799:2005 em sua totalidade foi feito.

A norma NBR ISO/IEC 17799:2005 retrata alguns fatores críticos de sucesso, levar em consideração estes fatores críticos foi preponderante para a execução dos trabalhos, pois procurou-se adequar-se aos requisitos apontados como fatores críticos, fatores como: ter uma política de segurança, possuir comprometimento e apoio dos níveis gerenciais da organização, fazer análise de risco, divulgação eficiente da política de segurança, e provisão de recursos.

Através dos dados levantados durante as atividades, constatou-se que das etapas metodológicas cumpridas, as que mais consumiram tempo para execução foram: a construção da Matriz de Análise de Riscos (vinte e um dias); e a confecção da Política de Segurança (sete dias).

No que se diz respeito a custos em recursos humanos, os dois tipos de profissionais que mais se envolveram e tiveram custos de hora trabalhada foram o *security officer* e a equipe de TI. Seguindo com terceiro maior custo de hora trabalhada, os representantes de cada setor chave do colégio envolvidos nas atividades propostas.

É importante saber que numero de integrantes da equipe de TI pode variar conforme as especificidades da organização em que se vai aplicar a metodologia de trabalho, caso uma organização ou colégio possua um grau de informatização alto ou um parque de informática extenso o número de integrantes requeridos aumenta, aumentando o custo deste recurso humano. Em compensação, com o aumento do número de integrantes da equipe de TI, se reduziria o tempo de cumprimento de algumas etapas como a construção da Matriz de Análise de Riscos (a equipe ajudaria o *security officer* nas pesquisas e estudos) e principalmente na implementação dos controles sugeridos na matriz.

5 CONCLUSÕES E TRABALHOS FUTUROS

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 discutiu um estudo de caso da implementação da norma NBR 17799:2005 para gerência de segurança da informação em colégios.

Segundo a norma NBR ISO/IEC 17799:2005, deve-se começar construindo uma Política de Segurança da Informação, para então estabelecer os requisitos de segurança da informação, objetivo que pode ser atingido realizando a análise de riscos; e consultando legislações, regulamentos e normas vigentes. Após a análise de riscos, é necessário realizar a escolha dos controles e implementá-los. Assim, a metodologia apresentada neste trabalho procurou acatar o que recomenda a NBR ISO/IEC 17799:2005 para implementação de seus controles, ou seja, a metodologia utilizada propõe a construção da Política de Segurança, aplicação de ferramentas como Mapeamento de Relevância, estudo de prioridades GUT e a construção de uma Matriz de Análise de Riscos, onde, com base nas ameaças, vulnerabilidades, probabilidade de ocorrência da ameaça e o impacto, pode-se analisar a implementação/escolha de um controle de segurança ou não.

Concluiu-se que o documento da Política de Segurança é o documento principal dentro da Gestão da Segurança da Informação de uma organização. Pois, no estudo de caso ela foi o documento de alto nível que representou o topo de uma pirâmide de outros documentos e procedimentos adotados no colégio. Ela foi construída com a finalidade de prover uma orientação e o apoio da direção da organização para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

Logo após a confecção, aprovação e divulgação da Política de Segurança do CMSM aos colaboradores, puderam-se notar o seguinte:

- maior apoio e atenção da direção e subdireção do colégio com relação a Segurança da Informação;
- um alinhamento do colégio com as normas e procedimentos de segurança, não só da política do colégio, como de outros procedimentos considerados corretos para segurança da informação;
- diminuição do número de máquinas recolhidas para a Seção de Informática para manutenção;

- definição de responsabilidade pelos ativos de TI;
- maior aderência a padrões nacionais de segurança (NBR ISO/IEC 17799:2005);
- mudança de comportamento dos usuários de recursos de TI no sentido do aumento da correta utilização dos recursos de TI; e
- aumento considerável do nível de conscientização da importância da Segurança da Informação por parte do público interno do colégio.

As etapas que mais demandaram tempo para execução foram a construção da Matriz de Análise de Riscos e a confecção da Política de Segurança. A Matriz de Análise de Riscos devido ao alto grau de complexidade e conhecimentos necessários para sua confecção, e a Política de Segurança pela sua grande importância dentro do processo de Gestão da Segurança da Informação.

Os dois tipos de profissionais que mais se envolveram e tiveram custos de hora trabalhada foram o *security officer* e a equipe de TI. O maior custo do s*ecurity officer* deve-se ao fato deste profissional, além de ser o responsável por todo o projeto de segurança, foi o que mais absorveu horas de trabalho e participou de todas as atividades. O alto custo da equipe de TI, deve-se ao fato de que depois do *security officer*, foi o tipo de profissional que mais se envolveu em atividades e seu custo também foi influenciado pela quantidade de profissionais envolvidos na equipe. A quantidade de profissionais que compõem uma equipe de TI é influenciada pelo grau de informatização e o tamanho do parque de informática que a organização possuir, pois quanto maior estes índices tanto maior deve ser a equipe.

Assumindo que o trabalho contempla os ativos da informação do nível tecnológico e de informática, o fato do *security officer* ser um especialista em TI foi de fundamental importância, pois muitos dos conceitos de segurança, recursos de TI, sistemas de informação, mecanismos de segurança já eram conhecidos por este profissional. Assim, caso o perfil do *security officer* não seja tecnológico, a necessidade de treinamento é fundamental, o que tende a aumentar o custo final.

Para os trabalhos futuros sugere-se a implementação da norma a todos os setores do colégio, tornando a segurança mais abrangente. Caso o colégio procure uma futura certificação, o emprego de empresa especializada em segurança para apoio e consultoria pode se tornar necessário.

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799**. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

_____. **NBR 17799**. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

BAKRY, Saad Haj., SALEH, Mohammad S. and ALRABIAH, Abdullah. **Using ISO 17799:2005 information security management: a STOPE view with six sigma approach.** International Journal of Network Management – 2007. v 17, p. 85-97, jun 2006.

BAKRY, S H and BAKRY, F H. **A strategic view for the development of e-business.** International Journal of Network Management – 2001. v 11, p. 103-112.

BDTD. **Biblioteca Digital de Teses e Dissertações.** Disponível em http://bdtd.ibict.br/bdtd/ Acesso em: 18 Dez 2006.

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

CARUSO, Carlos A. **A Segurança em Microinformática e em Redes Locais**. São Paulo. Editora: LTC, 1995 CUSTER, Helen; Windows NT .; São Paulo : Makron Books - 1993.

CASANAS, Alex D. Gonçalves; MACHADO, César de Souza. **O impacto da implementação da norma NBR ISO/IEC 17799.** 11 Mai 2006. Modulo Security Magazine. Disponível em http://www.modulo.com.br Acesso em: 11 Dez 2006.

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

CAVALCANTE, Sayonara de Medeiros. **Segurança da Informação no Correio Eletrônico baseada na ISO/IEC 17799: um estudo de caso em uma instituição de ensino superior, com foco no treinamento.** Dissertação de Mestrado – Universidade Federal do Rio Grande do Norte, Natal, 2003.

CERT.BR. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em http://www.cert.br/stats/incidentes/ Acesso em: 10 Dez 2007.

DEMO, Pedro. **Pesquisa e construção de conhecimento.** Rio de Janeiro: Tempo Brasileiro, 1996.

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

DUARTE, Carolina. **Normas internacionais em segurança da informação: Grandes mudanças na versão 2005 da ISO/IEC 17799.** 19 Jan 2006. Modulo Security Magazine. Disponível em http://www.modulo.com.br Acesso em: 30 Dez 2006.

FILHO, Ramiro Fernandes Rodrigues. **Proposta de Metodologia para a Elaboração de um Plano Diretor de Segurança da Informação.** Dissertação de Mestrado – Faculdades IBMEC, Rio de Janeiro, 2005.

FRIEDLOB, G. T. and PLEWA Jr. F. J., **Understanding Return on Investment.** Published by John Wiley & Sons, Inc. 1996.

GABBAY, Max Simon. **Fatores Influenciadores da Implementação de Ações de Gestão de Segurança da Informação: um estudo com Executivos e Gerentes de Tecnologia da Informação em empresas do Rio Grande do Norte.** Dissertação de Mestrado – Universidade Federal do Rio Grande do Norte, Natal, 2003.

GIL, Antonio C. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

GIL, Antonio de Loureito. **Auditoria de Computadores.** Editora Atlas, 2000.

HOLANDA, Roosevelt de. **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.

HUGHES, Larry J. Jr. **Actually Useful Internet Security Techniques**. Pratice Hall, 1997.

ISMS. **Information Security Management System (ISMS) International User Group Ltd.** Disponível em http://www.iso27001certificades.com Acesso em: 02 Mai 2007.

KALLAS, Tânia Maria Ribeiro de Bragança. **Planejamento Estratégico para Escola de Primeiro Grau.** Dissertação de Mestrado - Universidade Federal de Itajubá. 2004

KELLEY, Robert. **O Poder dos Seguidores: Como criar os verdadeiros líderes.** São Paulo: Siciliano, 1993.

KOUZES, James M. and POSNER, Barry Z. **O Desafio da Liderança**. Rio de Janeiro: Campus, 2003.

LEV, B. **Afiando os intangíveis.** Harvard Business Review, Volume 82, Número 6, Junho 2004.

LIMA, Luiz Fernando Ferreira de Medeiros. **Percepção de Segurança em Sistemas de Informação e sua relação com a qualidade percebida de Serviços, Perfil de Liderança e Perfil dos Seguidores, entre as Diretorias do INMETRO**. Dissertação de Mestrado Profissional em Sistemas de Gestão – Universidade Federal Fluminense, Niterói, 2006.

MACHADO, César de Souza. **Gerenciamento da Segurança da Informação no Teletrabalho.** Dissertação de Mestrado - Universidade Federal de Santa Catarina, Florianópolis, 2002.

_____. **FAQ sobre as normas BS 7799 e ISO 17799**. 24 Abr 2002, versão atualizada em 25 Fev 2005. Modulo Security. Disponível em http://www.modulo.com.br Acesso em: 18 Dez 2006.

MAY, Lauren and LANE, Tim. **A Model for Improving e-Security in Autralian Universities.** Journal of Theoretical and Applied Eletronic Commerce Research. v 1, p. 90-96, 2006.

MODULO SECURITY SOLUTIONS S.A. **10ª Pesquisa Nacional de Segurança da Informação.** 2006. Disponível em http://www.modulo.com.br Acesso em: 18 Jun 2007.

_____. **9ª Pesquisa Nacional de Segurança da Informação.** 2003. Disponível em http://www.modulo.com.br Acesso em: 12 Dez 2006.

_____. **2ª Pesquisa Nacional sobre o Perfil do Profissional de Segurança da Informação.** 2004. Disponível em http://www.modulo.com.br Acesso em: 12 Dez 2006.

MUKUND, Biju. **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.

NBSO. **Práticas de Segurança para Administradores de Redes Internet.** Versão 1.2 de 16 de maio de 2003.

PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. **Delivering Quality Service**. New York: The Free Press, 1990.

POPPER, Karl S. **A lógica da pesquisa científica.** 2 ed. São Paulo: Cultrix, 1975.

PYZDEK, T. **The Six Sigma Handbook.** McGraw-Hill. New York, 2003.

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

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

SCAMBRAY, Joel; SHEMA, Mike. **Segurança Completa contra Hackers: Aplicações Web**. Editora Futura, 2003.

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

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

ANEXOS

ANEXO A – Controles da Norma NBR ISO/IEC 17799:2005

Os controles da NBR ISO/IEC 17799:2005 são os seguintes (apresentados com a mesma numeração em que se encontram na norma):

5) Política de Segurança da Informação

5.1) Política de segurança da informação

5.1.1) Documentação da política de segurança da informação

5.1.2) Análise crítica da política de segurança da informação

6) Organizando a Segurança da Informação

6.1) Infra-estrutura da segurança da informação

6.1.1) Comprometimento da direção com a segurança da informação

6.1.2) Coordenação da segurança da informação

6.1.3) Atribuição de responsabilidades para a segurança da informação

6.1.4) Processo de autorização para os recursos de processamento da informação

6.1.5) Acordos de confidencialidade

6.1.6) Contato com autoridades

6.1.7) Contato com grupos especiais

6.1.8) Análise crítica independente de segurança da informação

6.2) Partes externas

6.2.1) Identificação dos riscos relacionados com partes externas

6.2.2) Identificando a segurança da informação, quando tratando com clientes

6.2.3) Identificando segurança da informação nos acordos com terceiros

7) Gestão de Ativos

7.1) Responsabilidade pelos ativos

7.1.1) Inventário dos ativos

7.1.2) Proprietário dos ativos

7.1.3) Uso aceitável dos ativos

7.2) Classificação da informação

7.2.1) Recomendações parar classificação

7.2.2) Rótulos e tratamento da informação

8) Segurança em Recursos Humanos

8.1) Antes da Contratação

8.1.1) Papéis e responsabilidades

8.1.2) Seleção

8.1.3) Termos e condições de contratação

8.2) Durante a contratação

8.2.1) Responsabilidades da direção

8.2.2) Concientização, educação e treinamento em segurança da informação

8.2.3) Processo disciplinar

8.3) Encerramento ou mudança da contratação

8.3.1) Encerramento de atividades

8.3.2) evolução de ativos

8.3.3) Retirada de direitos de acesso

9) Segurança Física e do Ambiente

9.1) Áreas seguras

9.1.1) Perímetro de segurança

9.1.2) Controles de entrada física

9.1.3) Segurança em escritórios, salas e instalações

9.1.4) Proteção contra ameaças externas e do meio ambiente

9.1.5) Trabalhando em áreas seguras

9.1.6) Acesso do público, áreas de entrega e de carregamento

9.2) Segurança de equipamentos

9.2.1) Instalação e proteção do equipamento

9.2.2) Utilidades

9.2.3) Segurança do cabeamento

9.2.4) Manutenção dos equipamentos

9.2.5) Segurança de equipamentos fora das dependências da organização

9.2.6) Reutilização e alienação segura de equipamentos

9.2.7) Remoção de propriedade

10) Gestão das Operações e Comunicações

10.1) Procedimentos e responsabilidades operacionais

10.1.1) Documentação dos procedimentos de operação

10.1.2) Gestão de mudanças

10.1.3) Segregação de funções

10.1.4) Separação dos recursos de desenvolvimento, teste e de produção

10.2) Gerenciamento de serviços terceirizados

10.2.1) Entrega de serviços

10.2.2) Monitoramento e análise crítica de serviços terceirizados

10.2.3) Gerenciamento de mudanças para serviços terceirizados

10.3) Planejamento e aceitação dos sistemas

10.3.1) Gestão de capacidade

10.3.2) Aceitação de sistemas

10.4) Proteção contra códigos maliciosos e códigos móveis

10.4.1) Controles contra códigos maliciosos

10.4.2) Controles contra códigos móveis

10.5) Cópias de segurança

10.5.1) Cópias de segurança da informação

10.6) Gerenciamento da segurança em redes

10.6.1) Controles de redes

10.6.2) Segurança dos serviços de redes

10.7) Manuseio de mídias

10.7.1) Gerenciamento de mídias removíveis

10.7.2) Descarte de mídias

10.7.3) Procedimentos para tratamento de informação

10.7.4) Segurança da documentação dos sistemas

10.8) Troca de informações

10.8.1) Políticas e procedimentos para a troca de informações

10.8.2) Acordos para a troca de informações

10.8.3) Mídias em trânsito

10.8.4) Mensagens eletrônicas

10.8.5) Sistemas de informação do negócio

10.9) Serviços de comércio eletrônico

10.9.1) Comércio eletrônico

10.9.2) Transações on-line

10.9.3) Informações publicamente disponíveis

10.10) Monitoramento

10.10.1) Registros de auditoria

10.10.2) Monitoramento do uso de sistema

10.10.3) Proteção das informações dos registros (log)

10.10.4) Registros (log) de administrador e operador

10.10.5) Registros (log) de falhas

10.10.6) Sincronização dos relógios

11) Controle de Acesso

11.1) Requisitos de negócio para controle de acesso

11.1.1) Política de controle de acesso

11.2) Gerenciamento de acesso do usuário

11.2.1) Gerenciamento de privilégios

11.2.2) Gerenciamento de senha do usuário

11.2.3) Análise crítica dos direitos de acesso de usuário

11.3) Responsabilidade dos usuários

11.3.1) Uso de senhas

11.3.2) Equipamento de usuário sem monitoração

11.3.3) Política de mesa limpa e tela limpa

11.4) Controle de acesso à rede

11.4.1) Política de uso dos serviços de rede

11.4.2) Autenticação para conexão externa do usuário

11.4.3) Identificação de equipamento em redes

11.4.4) Proteção e configuração de portas de diagnóstico remotas

11.4.5) Segregação de redes

11.4.6) Controle de conexão de rede

11.4.7) Controle de roteamento de redes

11.5) Controle de acesso ao sistema operacional

11.5.1) Procedimentos seguros de entrada no sistema (log-on)

11.5.2) Identificação e autenticação de usuário

11.5.3) Sistema de gerenciamento de senha

11.5.4) Uso de utilitários de sistema

11.5.5) Desconexão de terminal por inatividade

11.5.6) Limitação de horário de conexão

11.6) Controle de acesso à aplicação e à informação

11.6.1) Restrição de acesso à informação

11.6.2) Isolamento de sistemas sensíveis

11.7) Computação móvel e trabalho remoto

11.7.1) Computação e comunicação móvel

11.7.2) Trabalho remoto

12) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

12.1) Requisitos de segurança de sistemas de informação

12.1.1) Análise e especificação dos requisitos de segurança

12.2) Processamento correto nas aplicações

12.2.1) Validação dos dados de entrada

12.2.2) Controle do processamento interno

12.2.3) Integridade de mensagens

12.2.4) Validação de dados de saída

12.3) Controles criptográficos

12.3.1) Política para o uso de controles criptográficos

12.3.2) Gerenciamento das chaves

12.4) Segurança dos arquivos do sistema

12.4.1) Controle de software operacional

12.4.2) Proteção dos dados para teste de sistema

12.4.3) Controle de acesso ao código-fonte de programa

12.5) Segurança em processos de desenvolvimento e de suporte

12.5.1) Procedimentos parar controle de mudanças

12.5.2) Análise crítica técnica das aplicações após mudanças no sistema operacional

12.5.3) Restrições sobre mudanças em pacotes de software

12.5.4) Vazamento de informações

12.5.5) Desenvolvimento de terceirizado de software

12.6) Gestão de vulnerabilidades técnicas

12.6.1) Controle de vulnerabilidades técnicas

13) Gestão de Incidentes e Segurança da Informação

13.1) Notificação de fragilidades e eventos de segurança da informação

13.1.1) Notificação de eventos de segurança da informação

13.1.2) Notificando fragilidades de segurança da informação

13.2) Gestão de incidentes de segurança da informação e melhorias

13.2.1) Responsabilidades e procedimentos

13.2.2) Aprendendo com os incidentes de segurança da informação

13.2.3) Coleta de evidências

14) Gestão da Continuidade do Negócio;

14.1) Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

14.1.1) Incluindo segurança da informação no processo de gestão da continuidade de negócio

14.1.2) Continuidade de negócios e análise/ avaliação de riscos

14.1.3) Desenvolvimento e implantação de planos de continuidade relativos à segurança da informação

14.1.4) Estrutura do plano de continuidade do negócio

14.1.5) Testes, manutenção e reavaliação dos planos de continuidade do negócio

15) Conformidade

15.1) Conformidade com requisitos legais

15.1.1) Identificação da legislação vigente

15.1.2) Direitos de propriedade intelectual

15.1.3) Proteção de registros organizacionais

15.1.4) Proteção de dados e privacidade de informações pessoais

15.1.5) Prevenção de mau uso de recursos de processamento da informação

15.1.6) Regulamentação de controles de criptografia

15.2) Conformidade com normas e políticas de segurança da informação e conformidade técnica

15.2.1) Conformidade com as políticas e normas de segurança da informação

15.2.2) Verificação da conformidade técnica

15.3) Considerações quanto à auditoria de sistemas de informação

15.3.1) Controles de auditoria de sistemas de informação

15.3.2) Proteção de ferramentas de auditoria de sistemas de informação

APÊNDICES

APÊNDICE A – Política de Segurança

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEP - DEPA
COLEGIO MILITAR DE SANTA MARIA

PLANO DE SEGURANÇA DE INFORMÁTICA DO CMSM

1. INTRODUÇÃO

O presente plano tem como finalidade estabelecer as ações necessárias para assegurar certo nível de segurança de informações em informática, e também listar Normas e Recomendações de Utilização dos Recursos Computacionais e Serviços de Informática no CMSM.

2. PROCEDIMENTOS RELATIVOS À SEGURANÇA DA INFORMÁTICA

a. Procedimentos Gerais

1. A Subseção de Manutenção da Seção de Informática é a responsável pela manutenção dos equipamentos de informática de toda OM, não sendo permitido aos usuários a abertura de máquinas para solução de problemas.
2. A Subseção de Manutenção da Seção de Informática é a responsável "diagnóstico" para encaminhamento de equipamentos para manutenção externa via Almoxarifado.
3. Todo equipamento encaminhado para manutenção externa deve ter seu disco rígido removido pela Subseção de Manutenção da Seção de Informática.
4. As seções onde a Subseção de Manutenção da Seção de Informática verificar que a continuidade do trabalho é essencial devem ser equipadas com no-breaks e/ou geradores. O chefe de cada seção é responsável pela solicitação deste material à fiscalização administrativa.
5. Toda mídia destinada à reutilização deverá ter o seu conteúdo apagado de forma a impedir a recuperação dos dados anteriormente gravados na mesma.
6. A Subseção de Manutenção da Seção de Informática deve remover ou sobrepor informações sensíveis e softwares licenciados dos equipamentos inservíveis destinados à alienação.
7. Todo equipamento danificado contendo informações sensíveis deve ser analisado pela Subseção de Manutenção da Seção de Informática a qual determinará de destruição, reparação ou descarte do mesmo.

8. Qualquer instalação lógica (cabeamento) é de responsabilidade da Seção de Informática e deve obedecer às normas convencionadas de cabeamento estruturado e manter-se separada das redes elétricas.
9. A Seção de Informática deve instalar ou solicitar instalação por empresa capacitada de fibra ótica sempre que for necessária.
10. A Seção de Informática é responsável pela identificação de todos os pontos de rede.
11. Todos os equipamentos de conexão de rede (Hubs, Switches, Roteadores, etc) devem estar instalados em racks chaveados. Qualquer conexão a estes equipamentos deve ser feita somente com autorização da Seção de Informática.
12. O usuário que não possuir senha deve procurar o Administrador de Redes para seu cadastramento.
13. A Ajudância Geral deve informar à Seção de Informática a inclusão ou exclusão de militares e funcionários civis para atualização do cadastro de usuários da rede.
14. É proibida a utilização dos equipamentos por qualquer pessoa não cadastrada pela Seção Informática ou não autorizada pelo responsável pelo equipamento.
15. Devem ser estabelecidos níveis de acesso aos computadores, criando grupos de usuários. Deve ser definido um perfil de usuário para cada sistema a ser operado.
16. Os usuários devem alterar a própria senha junto a Seção de Informática e devem fazê-lo caso suspeitem que a sua senha foi "descoberta".
17. A periodicidade de troca da senha deve ser preferencialmente mensal. Caso não seja possível, deve ser feita no máximo trimestralmente.
18. A senha deve possuir no mínimo 06 caracteres.
19. A senha deve ser composta de uma combinação de caracteres maiúsculos e minúsculos, sinais e números, que deve ser fácil de lembrar, porém difícil de ser descoberta.
20. A senha não deve ser constituída de combinações óbvias de teclado, tais como 12345, asdfg.
21. Os usuários devem manter instalado e ativo em seus equipamentos o software antivírus padronizado pela OM.
22. O antivírus deve ser atualizado no mínimo semanalmente via rede ou internet.
23. Todo meio magnético de armazenamento de dados deve ser verificado pelo software antivírus antes de sua utilização.
24. Devem ser utilizados, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF, etc.
25. Funcionamentos estranhos ou suspeitos no sistema devem ser reportadas a Subseção de Manutenção da Seção de Informática, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.
26. Deve ser desabilitado no programa de e-mail a auto-execução de arquivos anexados às mensagens.
27. Cada usuário é responsável pela cópia dos seus dados para o servidor de arquivos para posterior backup.

28. Não havendo servidor de arquivos, os dados de interesse da organização devem ser armazenados, semanalmente ou quando houver necessidade, em mídias adequadas fora da seção onde constam os dados de origem.
29. As mídias removíveis utilizadas como memórias secundárias devem ser armazenadas em local protegido e distinto daquele onde se encontram os dados originais evitando qualquer dano e possibilitando a recuperação dos mesmos em caso de sinistro dos originais.
30. Cada usuário é responsável por manter criptografados todos os dados confidenciais que manipula.
31. É proibido ao usuário o consumo de quaisquer alimentos, bebidas ou cigarros junto aos equipamentos de informática.

b. Procedimentos para as estações de trabalho

1. É proibida a utilização dos equipamentos para atividades não relacionadas ao trabalho desenvolvido pelo usuário.
2. Havendo necessidade de instalação de qualquer software, o usuário deve solicitá-la ao chefe da sua seção que encaminhará a solicitação à Subseção de Manutenção da Seção de Informática.
3. O usuário deve efetuar o logoff sempre que a estação de trabalho não estiver sendo utilizada.
4. É proibido o armazenamento de qualquer tipo de software (MP3, filmes, fotos, etc.) sem a devida autorização dos seus proprietários, que configure violação de direitos autorais ou qualquer outro tipo de pirataria.
5. Dados de interesse particular podem ser armazenados localmente desde que não ultrapassem 20% da capacidade de armazenamento do equipamento.
6. O usuário que não possuir conexão com a rede deve fazer o backup de seus dados em disquete, CD ou mídia adequada para este fim pelo menos uma vez por semana ou quando a situação o exigir, testando-o após a confecção e guardando-o em local seguro.
7. O usuário que necessite compartilhar documentos deve efetuar o compartilhamento utilizando-se de senha a qual deve ser de conhecimento somente do usuário ou grupo de usuários que farão uso da informação compartilhada.
8. Todo compartilhamento deve ser desfeito logo após verificar-se que não há mais necessidade do mesmo.
9. A Subseção de Manutenção da Seção de Informática é responsável pelo bloqueio das configurações de rede nas estações de trabalho.

c. Procedimentos para Internet e Intranet

1. É proibida a instalação de programas para utilização da Internet sem controle de procedência e sem a autorização prévia da equipe de informática responsável por essa atividade.

2. É proibida a utilização dos recursos computacionais de Internet para fins políticos ou circulação de propagandas de qualquer natureza que não atendam às necessidades do serviço.
3. É proibida a utilização dos recursos computacionais de Internet para fins não condizentes com os princípios do EB, tais como visualizar, transferir, armazenar ou divulgar materiais pornográficos, eróticos, indecentes, ofensivos, etc.
4. É proibida a propagação de vírus de computador, programas invasores (worms) ou qualquer outra forma de programas de computador que causem danos, permanentes ou temporários, nos equipamentos dos destinatários.
5. É proibida a transmissão de tipos ou quantidades de dados que causem falhas em serviços ou equipamentos da rede interna ou da Internet, tais como MP3, fotos e executáveis.
6. É proibida a utilização da rede para tentar e/ou realizar acesso não autorizado a dispositivos localizados na rede interna ou na Internet.
7. É proibido forjar endereços de máquinas, de rede ou de correio eletrônico, na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria.
8. É proibido destruir ou corromperem dados e informações de outros usuários.
9. É proibido executar ações que visem a violar a privacidade de outros usuários.
10. É proibida a reprodução de material sem a prévia autorização do proprietário, violando Copyright ou direito autoral alheio.
11. É proibida a distribuição, via qualquer recurso computacional disponível, de quaisquer mensagens não solicitadas (SPAM) e mensagens em massa para o mesmo destinatário (mail bombing).
12. É proibida a utilização de termos agressivos ou de baixo calão.
13. É proibido tornar público o conteúdo de correspondência particular sem o consentimento de seu proprietário.
14. É proibido publicar ou enviar trabalhos de outras pessoas sem o seu consentimento expresso, violando os direitos autorais.
15. É proibido enviar mensagens com conteúdo sigiloso sem autorização ou sem a utilização da segurança criptográfica apropriada.
16. A Seção de Informática e o Oficial de Segurança das Informações são os responsáveis pela notificação de qualquer incidente ocorrido no uso da Internet e deverão:
    - incluir logs completos (com data, horário, timezone, endereço IP de origem, portas envolvidas, protocolo utilizado, etc) e qualquer outra informação que tenha feito parte da identificação do incidente e informar ao Centro de Inteligência do Exército.

<u>d. Procedimentos para Ambiente de Servidores</u>

1. O Administrador de Redes é responsável pela correta configuração do firewall.
2. Devem ser criadas regras de filtragem de sites que não são de interesse da organização e que possam bloquear a operação de serviços ou equipamentos, mensagens instantâneas (ICQ, IRC) e programas de distribuição de arquivos (Kaaza, Morpheus,

e-mule), permitindo o acesso a estes recursos somente a pessoal previamente cadastrado, cujas atividades desenvolvidas necessitem da utilização dos mesmos.

3. A Seção Informática deve manter um cadastro atualizado do pessoal que devido às atividades que desenvolve, necessita ter acesso a programas de trocas de mensagens e de distribuição de arquivos.
4. A Seção de Informática deve manter um cadastro atualizado de sites impróprios ou inadequados ao acesso por membros da OM.
5. Caso seja instalado algum tipo de proxy (como AnalogX, Wingate, WinProxy, Squid, etc) estes devem ser configurados para que apenas aceitem requisições partindo da rede interna.
6. Caso seja necessário compartilhar recursos como disco ou impressora entre máquinas da rede interna, deve-se tomar os devidos cuidados para que o firewall não permita que este compartilhamento seja visível pela Internet.
7. O RAS deve ser configurado de forma a aceitar conexão apenas de números telefônicos cadastrados.
8. Não deve ser instalado nenhum software desnecessário às atividades da seção.
9. Qualquer software só pode ser instalado em um servidor com a autorização do Administrador de Redes.
10. O Administrador de Redes deve zelar por manter ativos nos servidores somente os serviços de rede que estão sendo utilizados e desativar os demais.
11. A Seção de Informática é responsável pela auditoria dos servidores que apresentarem problemas, devendo corrigir o problema para que a falha não se repita.
12. Devem ser armazenados logs diários referentes às transações.
13. Apenas os Administradores de Rede devem ter conhecimento das senhas dos servidores.
14. A movimentação de qualquer dos integrantes da equipe de Administradores de Rede implica na modificação de todas as senhas de recursos e serviços dos servidores.
15. O backup dos dados do servidor é de responsabilidade do Administrador de Redes e deve ser feito pelo menos uma vez por semana em mídia adequada e armazenado em local seguro, fora da sala dos servidores.
16. As salas de servidores devem ser projetadas por pessoal capacitado de forma a proporcionar:
    - Isolamento quanto a ruídos e interferências provenientes de fontes externas;
    - Impermeabilização adequada para evitar infiltrações e vazamentos que possam vir a danificar os equipamentos;
    - Sistema de controle de temperatura e umidade de forma a proporcionar um ambiente adequado a operação dos equipamentos;
    - Fiação elétrica e lógica estruturada e embutida através da utilização de piso suspenso e outros recursos técnicos adequados a este fim;
    - Fornecimento de energia elétrica com tensão estável e monitorada, aterramento adequado e proteção contra surtos e descargas elétricas atmosféricas;

- Espaço adequado para o posicionamento de racks para instalação de hubs, switches, roteadores ou outros equipamentos de conexão à rede de forma a posicioná-los adequadamente e facilitar a manipulação e manutenção dos mesmos.

3. PLANO DE SEGURANÇA ORGÂNICA (SEÇÃO – INFORMÁTICA)

Finalidade: Padronizar as medidas a serem adotadas para utilização de recursos de informática pelos usuários, no âmbito do CMSM.

Ojetivos: Padronizar a correta utilização dos recursos de informática e protegê-los da perda de dados, programas ou acesso a informações por pessoas não autorizadas, bem como o acesso e a utilização dos serviços de informática (Internet, Intranet, estações de trabalho, etc) por parte dos usuários da OM de forma a obter-se um nível de segurança das informações eficaz e eficiente.

Execução: As medidas preventivas para utilização da informática estão agrupadas em quatro itens distintos (Medidas Preventivas Gerais, para Estações de Trabalho, para Internet e Intranet, e para Ambiente de Servidores), de acordo com sua abrangência:

a. Medidas Preventivas Gerais

1. Todos os recursos computacionais da OM devem ser usados somente para propósitos legais e autorizados.
2. Todo usuário é responsável pela segurança da informação que manipula, bem como pelos recursos computacionais ou de comunicações que utilizar.
3. A Subseção de Manutenção da Seção de Informática deve manter o controle sobre todos os equipamentos da OM.
4. Oficial de Segurança das Informações deve receber uma cópia do documento declaratório de todo o material de cada seção.
5. O acesso de pessoal aos laboratórios e salas de servidores deve ser controlado.
6. O acesso às seções que detém material de informática deve ser controlado.
7. O número de chaves das salas de servidores, laboratórios e seções que detêm material de informática deve ser limitado e constantemente controlado.
8. Fica proibida a utilização dos equipamentos por terceiros ou pessoas não autorizadas.
9. Os mecanismos físicos de segurança dos equipamentos devem ser sempre utilizados.
10. Qualquer manutenção de hardware só será permitida ao pessoal capacitado e habilitado da Subseção de Manutenção da Seção de Informática.
11. Sempre que o equipamento for para uma manutenção externa, o disco rígido deve ser retirado.
12. Deve haver conferências periódicas e inopinadas nos equipamentos.
13. Deve-se aplicar a correta utilização do RAS sempre que necessário.
14. A instalação do cabeamento de rede deve obedecer às normas convencionadas de cabeamento estruturado.

15. A instalação lógica deve ficar afastada das instalações elétricas para evitar interferências.
16. As instalações elétricas devem ser dimensionadas para suportar os equipamentos existentes no local, devendo ser estável e constante a corrente elétrica.
17. Toda a rede da OM deve ser aterrada, estabilizada e protegida contra descargas elétricas atmosféricas.
18. Devem ser utilizados no-breaks e/ou geradores nas seções onde a continuidade do trabalho é imprescindível.
19. É proibido o consumo de alimentos e bebidas junto aos equipamentos de informática.
20. Fica proibido o manuseio, envio, recepção e armazenamento de informações ou imagens de conteúdo ofensivo à força, pornográfico ou que denigra a imagem da pessoa, que incentivem a violência ou a discriminação de raça e credo, etc, independente do recurso ou meio utilizado.
21. Devem ser evitados o recebimento e a abertura de mensagens de correio eletrônico de origem duvidosa devido ao risco de contaminação por vírus.
22. Os arquivos temporários (de Internet, cookies, tmp, etc) devem ser eliminados periodicamente.
23. Todo usuário para ter acesso aos recursos computacionais deve possuir um login e senha.
24. A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
25. O tamanho mínimo da senha será estabelecido pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM.
26. A senha de boot não pode ser distribuída ou revelada.
27. Todo usuário demitido, afastado ou transferido da organização deve ter sua conta excluída.
28. Usuários devem ser cadastrados com os privilégios necessários para a função que executam.
29. Os usuários prestadores de serviço ou de teste devem possuir contas provisórias com data limite e estas devem ser imediatamente excluídas quando não forem mais utilizadas.
30. Dados de interesse da organização devem ser armazenados no servidor de arquivos para backups periódicos.
31. O compartilhamento de pastas deve ser feito somente para o usuário que necessite obter alguma informação da pasta em questão, sempre com senha.
32. Compartilhamentos devem ser desfeitos quando a informação necessária já foi adquirida.
33. Toda mídia removível utilizada como memória secundária deve ser mantida em um local seguro.
34. Toda informação deve ser adequadamente descartada quando de seu desuso.
35. Documentos confidenciais devem ser armazenados com o emprego de criptografia.

36. Documentos confidenciais que circulam na rede, interna ou externa, devem empregar criptografia.
37. Todos os equipamentos devem ter antivírus instalado e atualizado.
38. Nenhum software pode ser instalado sem autorização da Seção de Informática.
39. Todos os programas utilizados para o acesso aos recursos computacionais e documentos devem ser de procedência comprovada e estarem de acordo com as leis e normas de direitos autorais e de utilização, sendo de responsabilidade de cada usuário a garantia do cumprimento dessa prescrição.
40. Os softwares devem ser atualizados sempre que uma nova versão ou patch é lançado.

b. Medidas Preventivas para as Estações de Trabalho

1. Utilizar os microcomputadores estritamente para assuntos de trabalho.
2. Toda estação de trabalho deve possuir um sistema de senha que impossibilite sua utilização sem a identificação do usuário, mesmo para os serviços que independam de conexão à rede.
3. É obrigatório logar-se ao servidor para utilização da estação de trabalho.
4. Sempre que não for utilizada a estação de trabalho, a mesma deve estar desconectada da rede.
5. Não é permitido a instalação de qualquer software sem autorização.
6. É proibido o armazenamento de softwares que configure violação de direitos autorais ou qualquer outro tipo de pirataria.
7. Backup dos dados armazenados localmente no microcomputador é de responsabilidade do próprio usuário.
8. Todo backup deve ser armazenado em local seguro.

c. Medidas Preventivas para Internet e Intranet

1. Para cada usuário, deve ser estabelecido quais os recursos ou serviços que este poderá ter acesso, conforme a necessidade imposta pela natureza do trabalho que o usuário desenvolve.
2. A utilização de sites de bate-papo, programas de trocas de mensagens instantâneas ou programas de distribuição de arquivos devem ser restritos a pessoal previamente cadastrado cujas atividades desenvolvidas necessitem da utilização desse tipo de recurso.
3. Todas as mensagens eletrônicas enviadas por um usuário são de sua responsabilidade tanto quanto ao formato quanto ao conteúdo.
4. A largura de banda da rede para acesso externo deve ser adequada à necessidade da organização e estar disponível quando necessário.

d. Medidas Preventivas para Ambiente de Servidores

1. A sala dos servidores deve ser projetada visando proporcionar instalações e ambiente adequado à operação dos equipamentos nela contidos.
2. Toda a rede da organização deve ser isolada da rede externa por um firewall, adequadamente configurado.
3. Todas as transações efetuadas na rede devem ser monitoradas.
4. Nenhum software pode ser instalado sem autorização do Administrador da Rede.
5. Serviços essenciais da rede devem ser instalados em equipamentos exclusivos para este fim e com hardware adequado e compatível com a sua especificidade.
6. Serviços que servem como backup em caso de falha do principal devem ser instalados em equipamentos diferentes.
7. Serviços que não estão sendo utilizados devem ser desabilitados nos servidores.
8. Em caso de falha em algum serviço deve ser auditado o que provocou esta falha.
9. Deve ser utilizada uma senha diferente para cada serviço.
10. Todas as senhas de recursos e serviços dos servidores devem ser alteradas quando houver substituição de algum integrante da equipe de Administradores de Rede.
11. Deve ser utilizado um diretório diferente do padrão para armazenamento das senhas do servidor.
12. Deve ser efetuado o backup dos dados armazenados nos servidores periodicamente.
13. Todo backup deve ser armazenado em local seguro e distinto daquele onde se encontram os dados originais.

REFERÊNCIAS

- Portaria Nº 483, de 20 de Setembro de 2001 (IG 20-19), que aprova as Instruções Gerais de Segurança da Informação para o Exército Brasileiro).
- Norma Brasileira de Referência da ABNT (Associação Brasileira de Normas Técnicas) NBR ISO/IEC 17799 (Tecnologia da informação - Código de prática para a gestão da segurança da informação) de Agosto de 2005.
- Lei Nr. 3505 – Política de Segurança da Informação para órgãos do Governo Federal

Santa Maria, 28 de novembro de 2006.

APÊNDICE B – Matriz de Análise de Riscos

Ativos	Ameaças	Vulnerabilidades	Probabilidade	Impacto	Medidas
Banco de Dados	Perda de informações	Falta de Backup e backup armazenado em lugar inadequado	1	5	Deve ser efetuado o backup dos dados armazenados diário e guardados em lugar seguro.
SGE		Falta de Backup e backup armazenado em lugar inadequado	1	5	Deve ser efetuado o backup dos dados armazenados diário e guardados em lugar seguro.
SIMATEx		Falta de Backup e backup armazenado em lugar inadequado	2	2	Deve ser efetuado o backup dos dados armazenados semanalmente.
PROTWEB		Falta de Backup e backup armazenado em lugar inadequado	2	2	Deve ser efetuado o backup dos dados armazenados semanalmente.
Intranet		Falta de Backup e backup armazenado em lugar inadequado	2	2	Deve ser efetuado o backup dos dados armazenados semanalmente.
Banco de Dados	Demora para restabelecimento do serviço	Não possuir um plano de restabelecimento do serviço	3	4	Deve existir uma máquina reserva com o referido software para o pronto estabelecimento do serviço em caso de ocorrência de incidente.
SGE		Não possuir um plano de restabelecimento do serviço	3	4	Deve existir uma máquina reserva com o referido software para o pronto estabelecimento do serviço em caso de ocorrência de incidente.
SIMATEx		Não possuir um plano de restabelecimento do serviço	1	2	"Rodar" temporariamente o sistema em uma maquina tipo pc.
PROTWEB		Não possuir um plano de restabelecimento do serviço	2	1	"Rodar" temporariamente o sistema em uma maquina tipo pc.
Internet		Não possuir um plano de restabelecimento do serviço	3	3	Deve existir um modem substituto e um link com a internet sobressalente.
Intranet		Não possuir um plano de restabelecimento do serviço	1	1	Hospedar temporariamente a página da intranet em uma maquina tipo pc.
Rede	Acesso a sites indevidos	Falta de monitoração do usuário	3	1	Todas as transações efetuadas na rede devem ser monitoradas.
Servidor 1, 2 e 3		Falta de regras de filtragem de sites	4	1	Deve haver um mecanismo de bloqueio de sites impróprios ou que não são de interesse da organização.

Servidor 1, 2 e 3/ informação armazenada	Acesso físico indevido	Falta de controle das chaves da sala	5	4	A sala dos servidores deve ser projetadas visando proporcionar instalações e ambiente adequado à operação dos equipamentos nela contidos. O número de chaves das salas de servidores, laboratórios e seções que detêm material de informática deve ser limitado e constantemente controlado.
		Falta de procedimento operacional padrão para ingresso	5	4	O acesso de pessoal aos laboratórios e salas de servidores deve ser controlado
		Falta de mecanismo de segurança de travamento e registro de entrada de pessoal	5	4	O acesso de pessoal aos laboratórios e salas de servidores deve ser controlado
Rede	Acesso lógico indevido	Falta de procedimento formal de registro e cancelamento de usuários	5	1	Todo usuário demitido, afastado ou transferido da organização deve ter sua conta excluída.
		Pontos da rede em aberto	5	5	Não devem existir pontos de acesso abertos nos equipamentos que dão acesso à rede.
		Ausência de controle de concessão e uso de privilégios	0	4	Usuários devem ser cadastrados com os privilégios necessários para a função que executam.
		Falta de verificação dos logs	3	1	Todas as transações efetuadas na rede devem ser monitoradas.
		Ausência de bloqueio da estação	5	4	Deve ser utilizado um mecanismo temporizador para bloqueio das seções abertas e não em uso nos servidores.
Estação de trabalho		Instalação de pacotes/serviços não necessários e não monitorados	5	2	Não é permitido a instalação de qualquer software sem autorização.
		Não desconexão pelo usuário	5	4	Sempre que não for utilizada a estação de trabalho, a mesma deve estar desconectada da rede.
		Não utilização de patches de atualização	3	1	Utilizar os microcomputadores estritamente para assuntos de trabalho.
Servidor 1, 2 e 3		Instalação de pacotes/serviços não necessários e não monitorados	0	2	Nenhum software pode ser instalado sem autorização do Administrador da Rede.
		Não desconexão pelo usuário	5	4	Deve ser utilizado um diretório diferente do padrão para armazenamento das senhas do servidor.
		Não utilização de patches de atualização	3	1	Os softwares devem ser atualizados sempre que uma nova versão ou patch é lançado.
Estação de trabalho	Acesso lógico indevido	Login anônimo	2	1	É obrigatório logar-se ao servidor para utilização da estação de trabalho

		Ausência de bloqueio da estação	5	4	Toda estação de trabalho deve possuir um sistema de senha que impossibilite sua utilização sem a identificação do usuário, mesmo para os serviços que independam de conexão à rede
Estação de trabalho	Acesso remoto indevido	Modem nos equipamentos	0	4	Só poderão possuir modem (interno ou externo) ligados a uma linha telefônica externa os micros devidamente autorizados e cadastrados junto a Seção de Redes da Divisão de Telemática.
Servidor 1, 2 e 3		Não correta utilização do RAS	0	5	Deve-se aplicar a correta utilização do RAS sempre que necessário.
		Modem nas estações	0	4	Só poderão possuir modem (interno ou externo) ligados a uma linha telefônica externa os micros devidamente autorizados e cadastrados junto a Seção de Redes da Divisão de Telemática.
Rede	Demora para restabelecimento de serviço	Falta de plano de contingência	3	2	Deve existir uma máquina reserva para o pronto estabelecimento do serviço em caso de ocorrência de incidente.
Rede		Falta de planta baixa atualizada	5	2	A planta baixa da rede deve ser mantida atualizada.
		Falta de identificação de cabos	5	2	Todos os pontos de rede devem ser identificados nas duas extremidades.
Servidor	DNS	Utilização de um mesmo servidor com autoridade e recursivo	5	2	Serviços que servem como backup em caso de falha do principal devem ser instalados em equipamentos diferentes.
		Configuração do servidor DNS com excesso de privilégios	0	2	Serviços essenciais da rede devem ser instalados em equipamentos exclusivos para este fim e com hardware adequado e compatível com a sua especificidade
Servidor	Erros	Falta de conhecimento profundo do sistema operacional pelo administrador	3	4	Todos os usuários devem receber treinamento adequado e ter acesso a ferramentas e bibliografias necessárias ao correto desempenho de suas funções
Estação de trabalho	Hackers	Subversão de cookies	5	1	Os arquivos temporários (de Internet, cookies, tmp, etc) devem ser eliminados periodicamente.
Servidor 1, 2 e 3		Subversão de cookies	2	1	Os arquivos temporários (de Internet, cookies, tmp, etc) devem ser eliminados periodicamente.
Estação de trabalho	Hackers internos	Liberdade de acesso físico	5	4	O acesso às seções que detém material de informática deve ser controlado

		Acesso facilitado a dados / informações	4	4	O compartilhamento de pastas deve ser feito somente para o usuário que necessite obter alguma informação da pasta em questão, sempre com senha. Compartilhamentos devem ser desfeitos quando a informação necessária já foi adquirida.
Servidor 1, 2 e 3	Hackers: interceptação de comunicação	Utilização de serviços sem criptografia (telnet, ftp, rlogin, rsh, rexec)	3	5	Documentos confidenciais devem ser armazenados com o emprego de criptografia. Documentos confidenciais que circulam na rede, interna ou externa, devem empregar criptografia.
Servidor 1, 2 e3	Hackers: inundação de conexões TCP/UDP (servidor web)	Falta de contramedidas	3	2	A rede deve ser protegida de forma a impedir a ação de programas que fazem uso de códigos maliciosos do tipo cavalo de tróia, backdoors, worms, etc.
Rede	Hackers: adivinhação de senha	Falta de limite no nº de tentativas de logon	5	5	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
Servidor 1, 2 e3		Falta de criptografia no arquivo de senhas	2	5	Documentos confidenciais devem ser armazenados com o emprego de criptografia.
		Utilização do diretório padrão do arquivo de senhas	5	5	Todas as senhas de recursos e serviços dos servidores devem ser alteradas quando houver substituição de algum integrante da equipe de Administradores de Rede.
Servidor 1, 2 e3	Hackers: varredura de portas	Ausência de regra de filtragem no firewall	0	5	A rede deve ser protegida de forma a impedir a ação de programas que fazem uso de códigos maliciosos do tipo cavalo de tróia, backdoors, worms, etc.
Rede	Negação de serviço	Baixa largura de banda	5	2	A largura de banda da rede para acesso externo deve ser adequada à necessidade da organização e estar disponível quando necessário.
		Link único	5	2	A largura de banda da rede para acesso externo deve ser adequada à necessidade da organização e estar disponível quando necessário.
Estação de trabalho	Perda de informações	Falta de periodicidade de backup	5	4	Backup dos dados armazenados localmente no microcomputador é de responsabilidade do próprio usuário.

		Falta de definição dos dados a serem copiados	5	2	Dados de interesse da organização devem ser armazenados no servidor de arquivos para backups periódicos.
		Falta de local adequado para armazenamento do backup	5	5	Todo backup deve ser armazenado em local seguro.
		Falta de procedimento de verificação do backup	5	5	Deve haver um procedimento padrão pré-estabelecido para a confecção dos backups.
		Falta de procedimento para restauração	5	5	Deve haver um procedimento padrão pré-estabelecido para a restauração dos backups.
Servidor 1, 2 e 3		Falta de periodicidade de backup	0	4	Deve ser efetuado o backup dos dados armazenados nos servidores periodicamente.
		Falta de definição dos dados a serem copiados	0	2	Dados de interesse da organização devem ser armazenados no servidor de arquivos para backups periódicos.
		Falta de local adequado para armazenamento do backup	5	5	Todo backup deve ser armazenado em local seguro e distinto daquele onde se encontram os dados originais.
		Falta de procedimento de verificação do backup	5	5	Deve haver um procedimento padrão pré-estabelecido para a confecção dos backups.
		Falta de procedimento para restauração	5	5	Deve haver um procedimento padrão pré-estabelecido para a restauração dos backups.
Computadores (servidores e estações de trabalho) informação armazenada	Perda, dano ou comprometimento do equipamento	Falta de proteção contra relâmpagos e raios	5	2	Toda a rede da OM deve ser aterrada, estabilizada e protegida contra descargas elétricas atmosféricas.
		Falta de controle de acesso	5	5	O acesso às seções que detém material de informática deve ser controlado.
		Falta de extintores de incêndio e mecanismos de detecção de fumaça	5	5	Deve existir equipamentos de combate à incêndio em cada seção que possua equipamento de informática.
		Infiltrações de água	5	5	A sala dos servidores deve ser projetadas visando proporcionar instalações e ambiente adequado à operação dos equipamentos nela contidos.
		Falta de aterramento	5	5	Toda a rede da OM deve ser aterrada, estabilizada e protegida contra descargas elétricas atmosféricas.
		Falta de política específicas para alimentação e bebidas	5	5	É proibido o consumo de alimentos e bebidas junto aos equipamentos de informática.
		Falta de fontes de alimentação múltipla	5	2	As instalações elétricas devem ser dimensionadas para suportar os equipamentos existentes no local, devendo ser estável e constante a corrente elétrica.

		Falta ou subdimensionamento de no-break	5	2	Devem ser utilizados no-breaks e/ou geradores nas seções onde a continuidade do trabalho é imprescindível.
		Falta de gerador de reserva	5	2	Devem ser utilizados no-breaks e/ou geradores nas seções onde a continuidade do trabalho é imprescindível.
Estação de trabalho		Falta de controle dos equipamentos	5	1	Deve ser mantido um mapa de controle dos equipamentos.
Servidor 1, 2 e3		Falta de controle dos equipamentos	5	2	Deve ser mantido um mapa de controle dos equipamentos.
		Falta de controle de temperatura e umidade	3	2	A sala dos servidores deve ser projetadas visando proporcionar instalações e ambiente adequado à operação dos equipamentos nela contidos.
Servidor 1, 2 e3	Recebimento de SPAN	Falta de bloqueio do mail relay	0	1	Serviços que não estão sendo utilizados devem ser desabilitados nos servidores.
Cabeamento	Redução da vida útil do cabo	Não correta utilização de dutos ou conduites	5	2	A instalação lógica deve ficar afastada das instalações elétricas para evitar interferências.
Cabeamento	Rompimento de cabos	Instalação inadequada	3	2	A instalação do cabeamento de rede deve obedecer às normas convencionadas de cabeamento estruturado.
Estação de trabalho	Usuário insatisfeito / mal treinado	Falta de política de treinamento e valorização	5	4	Todos os usuários devem receber treinamento adequado e ter acesso a ferramentas e bibliografias necessárias ao correto desempenho de suas funções.
Rede	Utilização de senha por pessoa não autorizada	Falha na política de criação e alteração periodica de senhas	2	4	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
		Falta de manutenção de senhas dos usuários	2	1	Todo usuário para ter acesso aos recursos computacionais deve possuir um login e senha.
		Falta de atualização no cadastro de usuários da organização (desligamento)	2	1	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
		Utilização de senha padrão do sistema operacional	5	4	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.

Estação de trabalho		Engenharia social – tentativa de descoberta de informações pessoais do usuário	1	2	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
Informação armazenada	Vazamento de informação	Falta de criptografia das provas	0	5	Documentos confidenciais devem ser armazenados com o emprego de criptografia. Documentos confidenciais que circulam na rede, interna ou externa, devem empregar criptografia.
		Falta de criptografia dos documentos	5	4	Documentos confidenciais devem ser armazenados com o emprego de criptografia. Documentos confidenciais que circulam na rede, interna ou externa, devem empregar criptografia.
		Falta de criptografia no backup	5	5	Documentos confidenciais devem ser armazenados com o emprego de criptografia.
		Descarte inadequado de midias	5	5	Toda informação deve ser adequadamente descartada quando de seu desuso.
		Deslocamento de equipamentos para manutenção sem controle apropriado sobre os dados	5	5	Sempre que o equipamento for para uma manutenção externa, o disco rígido deve ser retirado.
Informação armazenada	Vazamento de informação	Compartilhamento e segurança de pastas / documentos indevido	5	4	O compartilhamento de pastas deve ser feito somente para o usuário que necessite obter alguma informação da pasta em questão, sempre com senha. Compartilhamentos devem ser desfeitos quando a informação necessária já foi adquirida.
Estação de trabalho	Vazamento de informação	Engenharia social – tentativa de descoberta de informações da organização	2	1	A política de senhas/privacidade será determinada pelo Administrador de Rede e/ou Oficial de Segurança das Informações da OM segundo as Normas Gerais de Ação de Informática.
Estação de trabalho	Vírus	Anti-vírus desatualizado	4	2	Todos os equipamentos devem ter antivírus instalado e atualizado.
		Utilização de discos removíveis	5	2	Todo usuário é responsável pela segurança da informação que manipula, bem como pelos recursos computacionais ou de comunicações que utilizar.

		Instalação de softwares não licenciados	3	1	Todos os programas utilizados para o acesso aos recursos computacionais e documentos devem ser de procedência comprovada e estarem de acordo com as leis e normas de direitos autorais e de utilização, sendo de responsabilidade de cada usuário a garantia do cumprimento dessa prescrição.
		Inexistencia de anti-vírus corporativo	5	2	Todos os equipamentos devem ter antivírus instalado e atualizado.
Servidor 1, 2 e 3		Anti-vírus desatualizado	4	2	Todos os equipamentos devem ter antivírus instalado e atualizado.
		Utilização de discos removíveis	5	2	Todo usuário é responsável pela segurança da informação que manipula, bem como pelos recursos computacionais ou de comunicações que utilizar.
		Instalação de softwares não licenciados	3	1	Todos os programas utilizados para o acesso aos recursos computacionais e documentos devem ser de procedência comprovada e estarem de acordo com as leis e normas de direitos autorais e de utilização, sendo de responsabilidade de cada usuário a garantia do cumprimento dessa prescrição.
		Inexistencia de anti-vírus corporativo	5	2	Todos os equipamentos devem ter antivírus instalado e atualizado.
		Ausência de regra de filtragem no firewall de arquivos executáveis	0	1	Devem ser evitados o recebimento e a abertura de mensagens de correio eletrônico de origem duvidosa devido ao risco de contaminação por vírus.

Impacto
0 - Impaco irrelevante
1 - Efeito pouco significativo, sem afetar a maioria dos processos de negócios da instituição
2 – Sistemas não disponíveis por um determinado período de tempo, podendo causar perda de credibilidade junto aos clientes e pequenas perdas financeiras
3 - Perda de credibilidade
4 - Efeitos desastrosos, porém sem comprometer a imagem da instituição
5 - Efeitos desastrosos, compremetendo a imagem da instituição

Ameaça
0 - Ameaça completamente improvável de ocorrer
1 - Probabilidade de ameaça ocorrer menos de uma vez por ano
2 - Probabilidade de ameaça ocorrer pelo menos uma vez por ano

3 - Probabilidade de ameaça ocorrer pelo menos uma vez por mês
4 - Probabilidade de ameaça ocorrer pelo menos uma vez por semana
5 - Probabilidade de ameaça ocorrer diariamente