UTILIZAÇÃO DAS NORMAS BSI 7799 NO GERENCIAMENTO DOS RISCOS EXISTENTES NOS SISTEMAS DE INFORMAÇÃO EMPRESARIAL

Silvana de Oliveira Tavares[1] (UNIB, Bolsista PIBIC/CNPq).
Álvaro Augusto Neto [2] (Orientador, ITA/IEC).

RESUMO

As informações são atualmente um dos principais ativos de que dispõem as organizações. Elas são essenciais para o gerenciamento de problemas relacionados com a estratégia de negócios e conseqüente competitividade ao se posicionar nos mercados.

Este trabalho tem por objetivo apresentar uma metodologia para avaliar e gerenciar os riscos, com relação à segurança das informações, a que estão submetidos os sistemas de informática de uma organização, visando a otimização dos procedimentos utilizados e a implementação de melhorias com relação a sua abordagem.

A metodologia proposta tem por base o conjunto de Normas BSI 7799, partes 1 e 2, desenvolvidas inicialmente pela *British Standards Institution*, e que posteriormente tiveram a sua primeira parte adotada pela International Standards Organization e pela Associação Brasileira de Normas Técnicas.

O método proposto pretende possibilitar às empresas uma análise do grau de riscos de segurança envolvidos em suas operações bem como, possibilitar posteriormente o seu gerenciamento. As empresas que pretendem implementar os padrões da norma poderão também utilizar esta metodologia para verificar o seu grau de adesão às prescrições das Normas.

[1] Aluna do Curso de Ciência da Computação, UNIB. **E-mail sotavares@hotmail.com**
[2] Pesquisador do ITA/IEC, Alvaro@comp.ita.br

MINISTÉRIO DA CIÊNCIA E TECNOLOGIA
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

UTILIZAÇÃO DA NORMA BSI 7799 NO GERENCIAMENTO DOS RISCOS EXISTENTES NOS SISTEMAS DE INFORMAÇÃO EMPRESARIAL

RELATÓRIO INICIAL DE PROJETO DE INICIAÇÃO CIENTÍFICA (PIBIC/CNPq/INPE)

Silvana Oliveira Tavares (UNIB, Bolsista PIBIC/CNPq)
E-mail: sotavares@hotmail.com

Álvaro Augusto Neto (ITA/IEC, Orientador)
E-mail: alvaro@comp.ita.br

Junho de 2004

Índice Analítico

UTILIZAÇÃO DAS NORMAS BSI 7799 NO GERENCIAMENTO DOS RISCOS EXISTENTES NOS SISTEMAS DE INFORMAÇÃO EMPRESARIAL

Silvana de Oliveira Tavares[1] (UNIB, Bolsista PIBIC/CNPq).

Álvaro Augusto Neto [2] (Orientador, ITA/IEC).

RESUMO

As informações são atualmente um dos principais ativos de que dispõem as organizações. Elas são essenciais para o gerenciamento de problemas relacionados com a estratégia de negócios e conseqüente competitividade ao se posicionar nos mercados.

Este trabalho tem por objetivo apresentar uma metodologia para avaliar e gerenciar os riscos, com relação a segurança das informações, a que estão submetidos os sistemas de informática de uma organização, visando a otimização dos procedimentos utilizados e a implementação de melhorias com relação a sua abordagem.

A metodologia proposta tem por base o conjunto de Normas BSI 7799, partes 1 e 2, desenvolvidas inicialmente pela *British Standards Institution*, e que posteriormente tiveram a sua primeira parte adotada pela International Standards Organization e pela Associação Brasileira de Normas Técnicas.

O método proposto pretende possibilitar às empresas uma análise do grau de riscos de segurança envolvidos em suas operações bem como, possibilitar posteriormente o seu gerenciamento. As empresas que pretendem implementar os padrões da norma poderão também utilizar esta metodologia para verificar o seu grau de adesão às prescrições das Normas.

[1] Aluna do Curso de Ciência da Computação, UNIB. **E-mail sotavares@hotmail.com**

[2] Pesquisador do ITA/IEC, Alvaro@comp.ita.br

CAPÍTULO 1 - INTRODUÇÃO

Em um livro de 1954, o Prof. J. Pinto Antunes, [1] já afirmava:

"Empresa é um dos regimes de produzir, onde alguém (empresário), por via contratual, utiliza os fatores da produção sob sua responsabilidade (riscos) a fim de obter uma utilidade, vendê-la no mercado e tirar, da diferença entre o custo da produção e o preço da venda, o maior proveito monetário possível".Em outras palavras, a empresa é uma organização de capital e trabalho, visando a produção ou mediação de bens e serviços para o mercado. O empresário, por seu turno, vem a ser o coordenador dessas atividades, assumindo todos os resultados e riscos delas provenientes.

Conforme esse conceito, a empresa é considerada um sistema aberto e complexo no qual entram recursos de diferentes naturezas, processa-os e os devolve transformados em bens ou serviços que serão utilizados pelos consumidores. A empresa interage com os fornecedores, clientes, governo, acionistas, bem como com concorrentes, economia, sociedade e política. A empresa se submete, assim, a pressões variadas, propiciadas pelo próprio ambiente em que se instala através de fatores que compõem as regras da competitividade, demandando uma melhor estratégia, para enfrentar as dificuldades originadas do próprio mercado.

Nesse contexto, a informação passa a ser a matéria matéria-prima mais importante para os empreendedores e gestores organizacionais basearem suas decisões sobre as melhores alternativas para o cumprimento de sua missão.

Assim, a informação apresenta grande importância por processar os dados derivados da execução das diversas atividades essenciais da empresa, gerando informações gerenciais valiosas para que o planejamento, operação e controle sejam feitos com o maior grau de eficácia possível.

Quando bem gerenciada, a área de informática beneficia a organização como um todo, ajudando os departamentos a atingirem suas metas de produção. Para isto, a empresa deve

disponibilizar em sua estrutura um sistema otimizado de informações que lhe dê a resposta eficaz para seu desempenho.

A informação se constitui hoje num importante ativo da empresa sendo de suma importância para o planejamento de estratégias competitivas, para manutenção em absoluto sigilo das informações sobre seus negócios.

Para manter o sigilo destes dados a empresa deve ter um método de comunicação integrado e seguro entre todos os seus setores, desde a direção até os departamentos de produção, fazendo com que os controles de dados, informações, experiências permitam o seu adequado posicionamento no mercado competitivo.

Aquelas empresas, cujo processamento de informações seja caótico, com programas de baixa qualidade e dados sem proteção, não terão condições adequadas de competir. A complexidade deve dar lugar à simplicidade, praticidade e procedimentos exatos e bem conhecidos.

Para preservar e garantir a confidencialidade, disponibilidade e integridade das informações, as empresas estão desenvolvendo e implantando métodos, técnicas e ferramentas voltadas para esse fim. Assume também um papel importante a conscientização com relação a segurança das informações fato por todos os usuários de seus sistemas informatizados.

Um ambiente de segurança bem implementado pode ser extremamente complexo e envolver vários produtos e técnicas. Por outro lado, este ambiente complexo pode ser bem administrado quando tem uma gerência dinâmica, que trabalhe dentro de um planejamento racional.

Dentro da atual visão gerencial, procura-se neste trabalho analisar as bases para implementação de melhorias na área de segurança, tendo como alicerce a Norma BSI 7799, tida como um dos padrões mais bem aceitos mundialmente pela área de segurança da informação.

1.1. Objetivo do Trabalho

Este trabalho tem por objetivo apresentar uma metodologia para avaliar e gerenciar os riscos, com relação a segurança das informações, a que estão submetidos os sistemas de informática de uma organização, visando a otimização dos procedimentos utilizados e a implementação de melhorias com relação a sua abordagem.

O método proposto pretende possibilitar às empresas uma análise do grau de riscos de segurança envolvidos em suas operações bem como, possibilitar posteriormente o seu gerenciamento. As empresas que pretendem implementar os padrões da norma poderão também utilizar esta metodologia para verificar o seu grau de adesão às prescrições das Normas.

1.2. Desenvolvimento da Pesquisa

A metodologia proposta tem por base o conjunto de Normas BSI 7799, partes 1 e 2, desenvolvidas inicialmente pela *British Standards Institution-BSI*, e que posteriormente tiveram a sua primeira parte adotada pela *International Standards Organization-ISO* e pela Associação Brasileira de Normas Técnicas-ABNT, além de outras fontes de informação relacionadas na bibliografia.

Através da metodologia proposta pretende-se implementar um conjunto homogêneo de procedimentos e de rotinas especificas que permitam gerenciar os riscos envolvidos e trazê-los para níveis toleráveis pelas organizações.

CAPÍTULO 2 – A NORMA BSI 7799

2.1. Introdução

Os padrões e normas foram criados como linguagem comum para todos. Em 1995, em busca de uma melhor estrutura para a área de segurança, foi desenvolvido no Reino Unido um padrão normativo que mais tarde veio a tornar-se um padrão mundial. Esta norma ficou conhecida pelo acrônimo BSI 7799. A norma BSI 7799 define métodos e práticas para as diversas áreas envolvidas pela segurança da informação.

A norma BSI 7799 é composta de duas partes. A primeira tem por objetivo analisar e implementar os procedimentos; à segunda, incumbe auditar e certificar a aplicação da primeira parte. A segunda parte da norma pode ser utilizada para certificar uma organização. Aplicando-se, portanto, a norma BSI 7799 em sua totalidade, a organização poderá ser certificada através do Sistema de Gerenciamento de Segurança da Informação.

A norma BSI 7799 passou a ser mais utilizada depois que sua primeira parte adotada pela International Standards Organization, passando a denominar-se ISO/IEC 17799:2000, tendo sido adotada por diversos países e traduzida para diversos idiomas, dentre os quais o português.

Vale ressaltar que o padrão ISO/IEC não é apenas a norma internacional de segurança de informação, mas uma metolodogia de trabalho, que vem sendo adotada por várias organizações a nível mundial.

2.2. História da Norma

Com o surgimento das máquinas compartilhadas (*time sharing*), tornou-se possível que diversas pessoas usassem simultaneamente o mesmo computador, surgindo problemas relacionados com o uso concomitante de seus recursos. Com o crescimento destes problemas, houve a necessidade de gerenciar os acessos, para evitar os problemas e dificuldades que surgiam devido ao compartilhamento de recursos e informações.

Com a evolução dos sistemas e sua posterior difusão, surgiu nos Estados Unidos o primeiro esforço para minimizar estes problemas, que resultou em um documento intitulado *Security Control for Computer System: Report of Defense Science Board Task Force on Computer Security*. Este documento, criado pelo Departamento de Defesa dos Estados Unidos, representou o inicio do processo de criação de um conjunto de regras para a segurança dos computadores. [2]

Contudo, este esforço não se deu somente por parte do Departamento de Defesa. Houve também o apoio da Agência Central de Inteligência, que patrocinou o desenvolvimento do primeiro sistema operacional que implementava políticas de segurança, chamado de ADEPT-50.

Em 1977, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar problemas de segurança de computadores, o qual deu origem ao DoD-Computer Security Initiative, que veio a desenvolver um centro para análise e avaliação da segurança das soluções utilizadas. O novo centro gerou a necessidade de criação de um conjunto de regras a serem utilizadas no processo de avaliação, que ficaram conhecidas como Orange Book. Graças às operações, e ao processo de criação do centro de avaliação e do Orange Book, foi possível a produção de uma grande quantidade de documentos técnicos, que representaram o primeiro passo na formação de uma norma completa sobre segurança de computadores.

O Orange Book tinha uma maneira simples de especificar o que deveria ser implementado e fornecido para um software, de sorte que o mesmo fosse classificado em níveis de segurança, e representou o marco inicial a partir do qual foram desenvolvidos diversos padrões de segurança com métodos e filosofia própria.

Em 1987 o Departamento de Indústria e Comércio do Reino Unido, criou o Centro de Segurança de Computação Comercial, que tinha por objetivo produzir um conjunto atualizado de práticas de segurança, com a finalidade de auxiliar usuários na implantação de sistemas de controle nas empresas. Deste esforço resultou o Código de Práticas para Usuários (*Users Code of Practice*), publicado em 1989. Este código foi avaliado por uma comissão ligada as indústrias britânicas. Após esta avaliação foi publicado um guia de segurança denominado

como "Um código de práticas para gerenciamento de segurança da informação" (*A code of pratice for information security management*), que após análise e algumas modificações, teve sua versão final editada em 1995, como o Padrão Britânico *(British Standard) BSI 7799: 1995.*

Com a criação da norma britânica, o interesse das grandes organizações ao redor do mundo foi despertado. Mesmo após sua revisão, antes da publicação final, ele ainda possuía certas limitações, pois era voltado apenas para as condições existentes no Reino Unido. Para superar estas limitações foram feitas outras revisões, que tiveram inicio em novembro de 1997 e foram concluídas em abril de 1998.

Nesta nova versão foi solicitada a colaboração de vários países, com a intenção de melhorar a norma e obter dois grandes objetivos: tornar-se mais flexível e ser amplamente divulgada. Em conseqüência a norma foi adotada por diversos países como França, Alemanha, Irlanda, Japão e Austrália.

Contudo, visando uma padronização mundial, houve um esforço para elaboração de uma norma mais atual, que não explorasse somente a questão da segurança de computadores, mas também uma segurança de toda e qualquer forma de informação. Este trabalho foi desenvolvido pela *IEC-International Electrotechnical Commission* da ISO.

Um ano após a última revisão em abril de 2000, a BSI 7799-1 foi submetida à ISO para se tornar um padrão internacional, cogitando-se a possibilidade de ser publicado dentro de um prazo de 12 meses. Em meados de outubro, a ISO aprovou a norma, tornando-a um padrão internacional, que foi publicado em dezembro de 2000.

Este resultado é apresentado como Norma Internacional de Segurança da Informação ISO/IEC-17799:2000, que possui uma versão aplicada aos países da língua portuguesa sob a denominação de NBR-ISO/IEC-17799.

Tanto a BSI 7799-1, quanto a ISO 17799 são normas para organizações, mas não definem a certificação de segurança. Elas apenas cumprem o primeiro objetivo de criar uma linguagem comum para melhor entendimento da estrutura de segurança de organizações. A

BSI 7799 parte 2, sem tradução para o português, tem em seu conteúdo as especificações usadas para a certificação.

Vale ressaltar que as normas enfatizam o fato que o fator relevante que permite diminuir os problemas de segurança são as questões gerenciais e ligadas a conduta humana.

2.3. Resumo da BSI 7799: 2000 - Parte 1

Em sua primeira parte, a Norma BSI 7799-1:2000 [10] traz conceitos e parâmetros que caracterizam os elementos que definem a segurança da informação.

Para a garantir a segurança da organização a Norma BSI 7799-1:2000, baseia-se em três pontos principais, confidencialidade, integridade e disponibilidade. Confidencialidade é a garantia de que a informação e somente será acessível para as pessoas autorizadas. A integridade garante a exatidão da informação e dos métodos de processamento. A disponibilidade visa garantir em os usuários autorizados obtenham acesso à informação e aos ativos correspondente sempre que isso for necessário.

A versão brasileira da norma, denominada NBR ISO/IEC 17799 [14] apresenta os seguintes tópicos principais :

2.3.1 - Objetivo da Norma

Fornece recomendações para a gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional. Sugere que as recomendações descritas na Norma sejam selecionadas e usadas de acordo com a legislação e as regulamentações vigentes.

2.3.2 - Política de segurança:

Deve prover à direção uma orientação e apoio para implementar medidas que conduzam à segurança da informação. Convém que a direção estabeleça uma política clara e

demonstre apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização.

2.3.3 - Segurança organizacional

Gerencia a segurança da informação na organização, é desejável que a estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Os fóruns apropriados de gerenciamento com liderança da direção devem ser estabelecidos para aprovar a política de segurança da informação. Se necessário, convém que uma fonte especializada em segurança da informação seja estabelecida e disponibilizada dentro da organização. Propõe que sejam mantidos contatos com especialistas de segurança externos, de forma a manter a organização atualizada com as tendências do mercado, monitorar os métodos de avaliação, além de fornecer apoio durante a ocorrência de incidentes de segurança.

2.3.4 - Classificação e controle dos ativos de informação

Manter a proteção adequada dos ativos da organização. Ë melhor que todos os principais ativos da informação sejam inventariados e tenham um proprietário responsável. O inventário dos ativos ajuda assegurar que a proteção esta sendo mantida de forma adequada. Convém que os proprietários dos principais ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A responsabilidade pela implementação dos controles pode ser delegada.

2.3.5 - Segurança através de pessoas

Busca reduzir os riscos de erros humanos, roubos, fraudes ou uso indevido das instalações e informações. Para tanto a responsabilidade de segurança deve ser atribuída desde a fase de recrutamento, incluída em contrato de trabalho e monitorada durante a sua vigência. Os candidatos em potencial devem ser devidamente analisados, especialmente se forem atuar em trabalhos sensíveis. Todos os funcionários e prestadores de serviço que utilizem as instalações de processamento da informação devem assinar um acordo de manutenção de sigilo.

2.3.6 - Segurança física e do ambiente

Busca prevenir o acesso não autorizado, danos e interferências às informações armazenadas em meios físicos da organização. Os recursos e instalações de processamento de informações críticas ou sensíveis de negócio devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle.

2.3.7 - Gerenciamento de operações e comunicações

Visa garantir a operação segura e correta dos recursos de processamento da informação. Aconselha que os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam claros e bem definidos. Isto abrange o desenvolvimento de procedimentos operacionais apropriados e de resposta a incidentes. Recomenda que se utilize a segregação de funções, quando apropriado, para reduzir o risco de uso negligente ou doloso dos sistemas.

2.3.8- Controle de acessos dos usuários

Busca prevenir acessos não autorizados aos sistemas de informação. Recomenda que procedimentos formais sejam estabelecidos para controlar a concessão de diretos de acesso aos sistemas de informação e serviços. Estabelece que os procedimentos devem cobrir todos os estágios do ciclo de vida de acesso de um usuário, indo desde o registro inicial de novos usuários até o registro final de exclusão dos usuários que não mais necessitam ter acesso aos sistemas de informação e serviços.

2.3.9 – Desenvolvimento e manutenção de sistemas.

Tem por objetivo garantir que a segurança seja parte integrante dos sistemas de informação. Isto inclui a infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelo usuário. O projeto e implementação dos processos de negócio que dão suporte às aplicações e aos serviços são cruciais para segurança. Os requisitos de segurança precisam ser identificados e acordados antes do desenvolvimento dos sistemas da informação.

2.3.10 - Gestão de continuidade de negócios

Busca impedir a interrupção das atividades do negócio e proteger recursos críticos contra efeitos de falhas ou desastres significativos. Sugere que o processo de gestão da continuidade seja implementado para reduzir, até um nível aceitável, a interrupção causada por desastres ou falhas da segurança que podem ser resultante de desastres naturais, acidentes, falhas de equipamentos e ações intencionais. Isto deve ser feito através da combinação de ações de prevenção e recuperação.

Recomenda que os planos de contingência sejam desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados dentro de um escala de tempo acaeitável pela organização. Salienta que tais planos sejam mantidos e testados de forma a se tornarem parte integrante de todos os processos gerenciais.

Salienta que a gestão de continuidade de negócio deve incluir controles para a identificação e redução de risco, a limitação das conseqüências dos danos do incidente e a garantia da recuperação tempestiva das operações vitais.

2.3.11. Analise critica da política de segurança e conformidade técnica.

Visa garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança. Convenciona que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares. Recomenda que tais análises críticas sejam executadas com bases nas políticas de segurança e que as plataformas técnicas e sistemas de informação seja auditados em conformidade com as normas de segurança implementadas

2.4 – Resumo da BSI 7799 –Parte 2: 2002

A norma BSI 7799-2:2002 [11], especifica os passos necessários que as organizações devem seguir para obter a certificação de acordo com a norma. Assim, enquanto a primeira parte analisa e organiza, a segunda implementa e valida a estrutura de segurança e melhoria do Sistema de Gestão de Segurança da Informação (SGSI)

Vale ressaltar que a Parte 1 da norma não determina que as empresas devam obter a certificação mencionada na Parte 2. No entanto, a certificação é um processo natural de implementação da norma nas empresas. A parte 2 irá autenticar os processos da primeira, especificando as exigências da melhoria do gerenciamento Sistema de Gestão de Segurança da Informação.

2.4.1 - Sistemas de Gerenciamento da Segurança da Informação (ISMS – Information Security Management System)

É um sistema de administração para estabelecer política e objetivos para a segurança da informação dentro do contexto do risco de negócio global da organização e os meios pelos quais estes objetivos podem se concluídos. Pode-se definir ISMS mais claramente como o recurso de avaliação e monitoramento da segurança da organização que serão auditados pela BSI 7799-2. [11]

Com o objetivo de obter credibilidade, as empresas buscam atualmente processos de gerência de segurança. Neste cenário, surgem os sistemas de gerenciamento da segurança da informação, que se tornam garantia de credibilidade da empresa junto aos clientes e parceiros.

O ISMS deve ser capaz de manter a informação sob o controle e de acordo com o especificado na política de segurança. Tanto as políticas, quanto os processos de gerência, devem ser orientados para a manutenção de alguns atributos da informação, com o objetivo de protegê-la contra as ameaças de origem interna e externa causadas por fenômenos da natureza ou humanos..

2.4. 2 - Elaboração do ISMS

A norma requer a elaboração de um esquema que mostre como monitorar e controlar a segurança, minimizando os riscos e garantindo que os controles aplicados estejam de acordo com as necessidades.

O ISMS será o processo a ser auditado de acordo com a norma BS 7799-2, através de métodos específicos e próprios de auditoria. Para isso, as entidades certificadoras enviam

auditores formados pela BSI, que analisam, checam e agem sobre os procedimentos que foram aplicados na primeira parte da norma.

Não só a parte 2 como a norma em geral pode ser comparada ao processo de gestão, chamado de ciclo do PDCA, (Plan, Do, Check, Action), ou seja, planejar, executar, verificar, agir. Este ciclo de gerenciamento bastante utilizado pelas empresas que implementam a gestão pela qualidade total. Alguns de seus precursores foram Deming, Juran, Crosby e entre os principais conceitos envolvidos pode-se citar:

- Segundo Deming a gestão pela qualidade total baseia-se na melhoria de produtos e serviços através da redução das incertezas e variações;

- Juran apregoa que a satisfação do cliente é resultante de um desempenho excepcional do produto, livre de problemas, defeitos e deficiências.

- Segundo Crosby, não existem problemas devido a qualidade e sim, com a falta dela. Segundo o autor, não existe economia com a falta de qualidade, pois fazer o trabalho certo desde a primeira vez é sempre mais barato. [5]

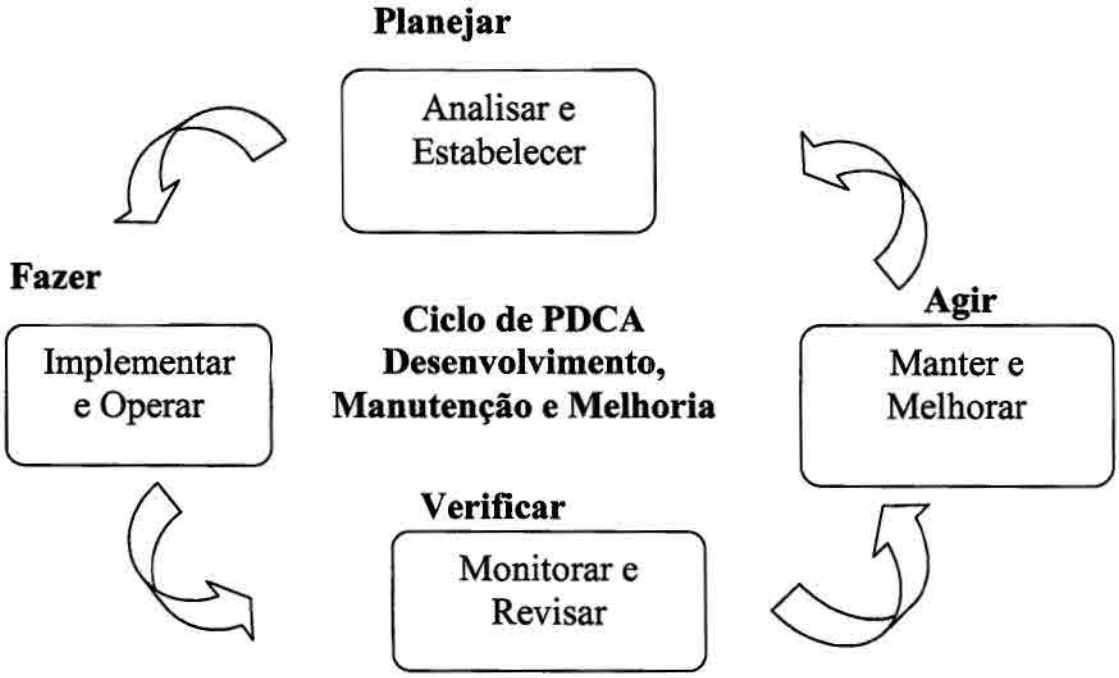

Figura 1- Modelo PDCA aplicado ao processos de melhoria

CAPITULO 3 – A METODOLOGIA DA BS-7799:2

A metodologia da BSI-7799:2 [11], divide-se em seis partes:

3.1 – Política de Segurança da Informação

Reflete todo o direcionamento da empresa relacionado com a informação e seus valores. Este documento deve destacar claramente as informações vitais para a empresa, e recomenda-se que nele seja definida a classificação e o valor das informações. Sua implantação deve contar com o apoio e participação da alta administração da empresa, de forma que se tenham garantias de que as regras da política não serão quebradas.

3.2 – Escopo

Nesta etapa, deve-se definir qual a abrangência do Sistema de Gerenciamento da Segurança da Informação, para que não haja extrapolação de suas atribuições. Deve-se montar uma estrutura para que se possa ter melhoria contínua nos procedimentos gerenciais da metodologia.

3.3 – Análise de Risco

Após rever as políticas e criar os escopos, há a necessidade de efetuar uma análise dos riscos de perda da confidencialidade, disponibilidade e integridade dos ativos. Nesta fase deve-se considerar diversos aspectos que possam ser classificados como ameaças à segurança da empresa.

3.4. - Gerenciamento de Risco

É a fase que define as ações e os recursos utilizados para gerenciar os riscos mais críticos. Além das ferramentas tecnológicas que deverão ser utilizadas para amenizar a ocorrência do risco, devem ser levadas em consideração a colaboração e conscientização dos recursos humanos. Esta fase é essencial para um bom plano de continuidade de negócios e deve ser muito bem elaborado.

3.5 – Escolha dos controles de segurança

Baseado na gerência de riscos e na NBR ISO/IEC 17799[14], deve-se escolher quais os controles que serão utilizados para a preservação da integridade, disponibilidade e confidencialidade das informações. A BSI 7799-2 [11] oferece uma grande quantidade de sugestões de como implantar e gerenciar cada controle.

3.6 – Definição de aplicabilidade dos controles

Nesta etapa, deve-se declarar quais os controles escolhidos e sua aplicabilidade dentro da empresa e do seu ambiente. Esta justificativa é muito importante para que fique claro porque os controles que foram escolhidos não foram excluídos das novas regras da empresa.

CAPÍTULO 4 – GESTÃO DE RISCOS

4.1 – Riscos

Toda empresa, todo negócio, tem por objetivo primeiro a obtenção do lucro, que com sorte aumenta seu patrimônio e capital, gerando assim riqueza que lhe possibilitem a continuidade e o crescimento de suas atividades. Desse modo, o risco e o retorno são os pontos cruciais que o administrador tem de enfrentar em suas decisões de avaliação e orçamento de capital. Dessa análise decorre o resultado positivo ou negativo do investimento realizado. Em suma, são a base para a tomada de decisões racionais e inteligentes.

A análise de risco e retorno é sempre medida sob uma visão financeira e de orçamento do capital. Assim, quanto maior o risco, maior a taxa de retorno; quanto menor o risco, menor a taxa de retorno. Risco é uma medida inconstante dos retornos e dos resultados futuros. O risco é assim mensurado pelo grau de inconstância associada aos retornos esperados. O risco pode ser definido como o desvio dos resultados esperados. Uma definição mais clara de ativo: são elementos aos quais a organização atribui valor e desta forma requerem proteção.

Outro elemento de análise de risco é a determinação das probabilidades. Estas vão mostrar ao empresário as chances ou promessas de sucesso de um evento ocorrer. Quando se trata de uma inovação, fica difícil ao administrador estabelecer as probabilidades, que são quase nulas, porque não existem parâmetros anteriores de ocorrência. Suas observações devem partir do ponto zero e as ocorrências serão anotadas conforme os intervalos de tempo em que acontecerem para evitar possíveis vulnerabilidades.

Os riscos da indústria e da companhia são avaliados levando-se em consideração diversos fatores, tais como solidez, oscilações na aquisição de matéria-prima, a modernização industrial, riscos ambientais e sociais, sujeição a legislações rígidas pertinentes a poluição ambiental, crises políticas internas e informações. Tudo isso pode levar a uma situação de aumentos de custos, inviabilizando o resultado positivo das empresas.

Existe, pois, uma interação de forças que influem nas relações entre retorno e riscos externos a serem consideradas nas estratégias de investimento de uma empresa para que possa minimizar seus riscos e maximizar seus retornos.

Até bem pouco tempo, a avaliação do risco era realizada pelo empresário sob a ótica restrita do volume de capital investido em projetos de natureza financeira. A atenção estava voltada apenas para os ativos financeiros. Com a mudança da visão empresarial, em que a matéria-prima voltou-se para a área do conhecimento, o direcionamento do empreendedor passou a abranger outros elementos da empresa para a elaboração do orçamento financeiro. Fazem parte de sua avaliação, o risco e retorno de capital, a parte física, os ativos fixos das empresas, e as informações industriais necessárias para a estruturação de sua estratégia competitiva.

O risco é, então, uma ocorrência que pode afetar os negócios e impedir que determinados objetivos sejam alcançados. Sua existência se alicerça com o surgimento de uma ameaça em potencial causando algum dano ou apresentando alto índice de probabilidade de ocorrência. Fazendo-se presente no ambiente computacional, em face da grande importância que a informação tem hoje no contexto empresarial como verdadeiro ativo estratégico para a organização.

A gestão de risco é, com certeza, a mais importante responsabilidade dos atos financeiros das empresas. Na área da informática, diante do crescimento dos problemas causados pela falta de segurança, o empreendedor está dando prioridade aos investimentos maiores na proteção de suas informações, hoje tão importante quanto às aplicações financeiras de mercado.

Podemos considerar que a análise de risco é peça fundamental para obtenção da qualidade de um programa de segurança, pois ajudará a identificar todos os pontos críticos e falhos de proteção em todos os processos, configurações, documentos, enfim, tudo que possa ser valioso para a atividade da empresa.

Essa atividade fornecerá diretrizes para a identificação das medidas de segurança necessárias para que o ambiente possa atingir um excelente nível de segurança. Conforme menciona Nilson Moreira. [7]

"a análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios. Através da aplicação desse processo é possível determinar as propriedades de ação em função do risco identificado para que seja atingido o nível de segurança desejado pela Organização. Proporciona também informações para que se possa identificar antecipadamente o tamanho e o tipo de investimento necessário para prevenir os impactos na Organização causados pela perda ou indisponibilidade dos recurso fundamentais para o negócio."

Como todos os ativos da empresa estão sujeitos a vulnerabilidades, em maior ou menor escala, isto pode significar riscos para a empresa, resultando muitas vezes de falhas nos seus controles.

Por outro lado, as ameaças exploram as vulnerabilidades existentes que decorrem de falhas de configurações, inexistência de proteção adequada, ou até mesmo falha humana.

O gerenciamento de riscos é um processo contínuo, que não termina com a implantação de uma medida de segurança. Através de monitoração direta e constante, é possível identificar onde foi bem sucedida e onde precisa de ajustes.

4.2. - Ativos:

Ativos são os elementos que manipulam, direta ou indiretamente, uma informação, inclusive a própria informação dentro de uma Organização, e é isso que deve ser protegido contra ameaças para que os processos funcionem corretamente.

Uma definição mais clara de ativo é que são elementos aos quais a organização atribui valor e desta forma requererem proteção.

Por outro lado, as ameaças exploram as vulnerabilidades existentes que decorrem de falhas de configurações, inexistência de proteção adequada, ou até mesmo falha humana.

O gerenciamento de riscos é um processo continuo, que não termina com a implantação de uma medida de segurança. Através de monitoração direta e constante, é possível identificar onde foi bem sucedida e onde precisa de ajustes.

4.3 – Vulnerabilidades

O significado da palavra "vulnerabilidade" poderá esclarecer bem o que precisa ser avaliado, e resolvido dentro da questão da segurança da informação:

vulnerabilidade : s. f. Qualidade ou estado de vulnerável. [13]

vulnerável: adj. m. e f. 1. Que pode ser vulnerado. 2. Diz-se do lado fraco de um assunto ou questão, e do ponto por onde alguém pode ser atacado ou ferido. [13]

Vulnerabilidade na área de informática é uma condição existente em software ou hardware que pode resultar em perda de confidencialidade, disponibilidade ou integridade das informações, ou apenas podemos dizer que é uma falha de segurança que pode ser explorada por ataques.

Uma falha em um processo ou em um sistema é uma porta aberta para um hacker efetuar uma invasão. Como conseqüência desse fato, os dados criptografados de uma empresa precisam ser mantidos em rede privada e de preferência com suas chaves trocadas de tempo em tempo.

Um ataque de Hacker é muito parecido com os procedimentos de prevenção do ataque, porque um hacker ou um cracker constrói uma metodologia de ataque antes de invadir um sistema. Ele encontra um alvo, planeja o ataque, realiza o ato e depois foge.

Bruce Schneier,[12] descreve a metodologia de ataque da seguinte maneira:

"Em geral, existem cinco etapas para um ataque bem sucedido":

1. *Identificar o alvo especifico que será atacado e coletar informações sobre esse alvo;*
2. *Analisar as informações e identificar uma vulnerabilidade no alvo, que realizará os objetivos do ataque;*
3. *Obter um nível de acesso apropriado ao alvo;*
4. *Realizar o ataque no alvo;*
5. *Completar o ataque, o que pode incluir a eliminação da evidencia do ataque, evitando retaliação"*

Com essa definição, pode-se ver claramente que as duas primeiras etapas são de pesquisas; já as três últimas envolvem o risco que o hacker corre ao preparar um ataque e não ser bem sucedido.

Hoje em dia, as ferramentas que os hackers usam estão tão desenvolvidas quanto as ferramentas que são usadas pelas empresas para se defender. Existem até hackers especializados em buscar informações em eventos, congressos, festas, devido ao fato das pessoas estarem mais propensas a liberar as informações.

O hacker acredita que fica mais fácil obter estas informações, ou analisar uma pessoa e deduzir suas senhas ou outras informações porque normalmente nestas ocasiões ocorrem troca de informações informais, como empresa que trabalha, com que banco trabalha, ou situações que ocorrem no cotidiano. Por causa destas situações é que os bancos ou empresas solicitam aos seus clientes ou funcionários que não usem senhas que começam com números 0 (zero) e 1 (um), com datas de nascimento, números da residência e telefônicos.

Portanto Vulnerabilidade é este elo fraco que os sistemas ou processos têm. Localizar esta vulnerabilidade na segurança é apenas uma etapa em direção à sua exploração.

CAPÍTULO 5 – DESENVOLVIMENTO DA METODOLOGIA

A partir da aplicação dos procedimentos da norma numa organização do setor de serviços, pretende-se desenvolver uma metodologia prática para avaliar e gerenciar os riscos com relação a segurança das informações, a que estão submetidos os sistemas de informática de uma organização, visando a otimização dos procedimentos utilizados e a implementação de melhorias com relação a sua abordagem, baseada no modelo PDCA descrito anteriormente.

O desenvolvimento dessa metodologia será objeto das próximas etapas deste trabalho.

CAPÍTULO 6– CONCLUSÕES E RECOMENDAÇÕES INICIAIS

O mundo tem passado por profundas mudanças em todas as áreas: política, cultural, social, tecnológica e econômica. As organizações são afetadas por todas essas mudanças. Por isto, elas devem se adequar-se aos novos tempos, inovando seus produtos e reavaliando seu papel diante deste mercado.

Qualidade, eficiência e eficácia no ambiente competitivo, se tornaram uma questão de extrema necessidade. Sem essas características, torna-se difícil, se não impossível, permanecer num mercado altamente competitivo e seletivo onde qualidade, preço e serviços fazem o diferencial. Dentro desta realidade as empresas abandonaram seus antigos modelos, aceitando novos desafios para se manter no mercado.

Neste cenário, verifica-se que qualidade e produtividade são requisitos básicos para satisfazer o cliente em termos de produtos/serviços. Para estabelecer preços competitivos as organizações buscaram assimilar essas novidades e mudar suas culturas e procedimentos para continuar operando nesse novo cenário.

Os conceitos de qualidade e produtividade reforçaram a idéia de que a empresa deve ser vista como um sistema integrado, não podendo haver diferenças entre seus setores, pois as metas e os objetivos serão obtidos por meio de planejamento, execução, checagem e controle dos recursos do sistema.

Este trabalho ressalta as funções da administração representadas pela implantação de um bom sistema de informação para fundamentar o processo de tomada de decisão nas organizações. Sem os dados e demais ativos bem protegidos, sem procedimentos, política de segurança bem elaborada e construção de uma conduta adequada não é possível construir uma boa estrutura empresarial.

Sendo assim, o setor de Informática tem uma importância impar no fornecimento de informações gerenciais, não somente de natureza financeira como também de natureza física, fazendo parte integrante e indissociável do planejamento estratégico, comercial e financeiro

de qualquer empresa moderna. Por isso é certo afirmar que a informação é um verdadeiro ativo do empresário.

O estudo realizado propiciou o reconhecimento de que o setor de informática, é a fonte geradora desses dados, identificando, mensurando, registrando e comunicando informações úteis ao gerenciamento e ao processo decisivo e de controle.

A necessidade da implantação de uma política de segurança da informação ficou bem nítida em nosso trabalho. Nesse aspecto destaca-se a valiosa contribuição que a Norma Internacional BSI 7799 pode dar ao empresário, tanto na proteção do conjunto de suas informações empresariais, essenciais para o planejamento e desenvolvimento das atividades industriais, como na condição de ferramenta para a construção de estratégias competitivas no mercado moderno.

Desta maneira, consideramos que, dando continuidade ao nosso trabalho, podemos sugerir um estudo mais aprofundado junto às empresas, por meio de pesquisa de campo, para avaliar melhor o nível de demanda das informações e sua aplicação como ferramenta gerencial. Também será interessante aprofundar os estudos no sentido de pesquisar, principalmente entre as empresas de pequeno e médio porte, o benefício trazido, ou não, pelo avanço tecnológico no campo eletrônico, para o desenvolvimento do sistema de informação e a implantação de política de segurança com base em padrões de normas internacionais.

BIBLIOGRAFIA

[1] ANTUNES, J. Pinto, *A Produção Sob o Regime da Empresa*, Editora José Bushatsky – São Paulo - 1954

[2] AMARAL, Marcos Prado, *Segurança da Informação em Ambientes Computacionais Complexos: uma Abordagem Baseada na Gestão de Projetos*, disponível on-line no site da Modulo www.modulo.com.br - São Paulo - 2001

[3] NBR, I*nformação e documentação: referencias: elaboração,* Associação Brasileira de Normas Técnicas – Rio de Janeiro – 2001

[4] BASTOS, Alberto, *Gerenciando a Segurança das Informações nas Empresas*, disponível on-line no site da Modulo, www.modulo.com.br - São Paulo - 1998

[5] CHIAVENATO, Idalberto, *Introdução à Teoria Geral da Administração,* 4ª Edição, Editora Makron Books - São Paulo

[6] FIGUEREDO, Leonardo Soares, *Segurança da Tecnologia da Informação*, disponível on-line no site da Módulo, www.modulo.com.br - São Paulo - 2002

[7] MOREIRA, Nilson Stringasci , *Segurança Mínima - Uma visão Cooperativa da Segurança de Informações*, Axcel – Rio de Janeiro - 2001

[8] NAKAMURA, Emilio Tissato, *Segurança de Redes em Ambientes Cooperativos,* Futura São Paulo - 2003

[9] AUGUSTO, Álvaro Neto, *Uma Metodologia para Avaliação da Segurança da Informação*, IN: Anais de I Encontro de Iniciação Cientifica e Pós-Graduação do ITA-ENCITA - São José dos Campos - 1995.

[10] BSI 7799-1:2000,*Information Security Management – Part 1: Code of Practice for Information Security Management*, British Standards Institution – Londres - 2000

[11] BSI 7799-2:2002, *Information Security Management – Part 2: Specification for Information Security Management Systems*, British Standards Institution – Londres - 2002

[12] SCHNEIER, Bruce, *Segurança. Com Segredos e Mentiras Sobre a Proteção na Vida Digital*, Campus – Rio de Janeiro – 2001

[13] FERREIRA, Aurélio Buarque de Holanda, *Dicionário Aurélio Eletrônico-Século XXI*, Versão 3.0, Lexikon Informática - 1999.

[14] NBR/IEC ISO/IEC 17799, *Tecnologia da Informação – Código de Prática para a Gestão da Segurança da Informação,* Associação Brasileira de Normas Técnicas – Rio de Janeiro – 2001