UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
MESTRADO PROFISSIONALIZANTE EM ENGENHARIA

SISTEMA DE GERENCIAMENTO DE SEGURANÇA DE INFORMAÇÕES: PROCESSO DE AUDITORIA

Fábio Antonio Pizzoli

Porto Alegre
2004

FÁBIO ANTONIO PIZZOLI

SISTEMA DE GERENCIAMENTO DE SEGURANÇA DE INFORMAÇÕES: PROCESSO DE AUDITORIA

Trabalho de Conclusão do Curso de Mestrado Profissionalizante em Engenharia como requisito parcial à obtenção do título de Mestre em Engenharia – modalidade Profissionalizante – Ênfase: Qualidade e Gerência de Serviços.

Orientador: Leonardo Rocha de Oliveira, Ph.D.

Porto Alegre
2004

Este Trabalho de Conclusão foi analisado e julgado adequado para a obtenção do título de Mestre em Engenharia e aprovado em sua forma final pelo Orientador e pelo Coordenador do Mestrado Profissionalizante em Engenharia, Escola de Engenharia – Universidade Federal do Rio Grande do Sul.

_____

Prof. Leonardo Rocha de Oliveira, Ph.D.
Escola de Engenharia / UFRGS
Orientador

_____

Prof[a]. Helena Beatriz Bettella Cybis, Dra.
Coordenadora MP/Escola de
Engenharia/UFRGS

Banca Examinadora:

Cláudio José Müller, Dr.
Prof. PPGEP/UFRGS

João Dornelles Junior, Dr.
Prof. PUCRS / RS

Mirian Oliveira, Dr[a].
Prof[a]. PUCRS / RS

Este trabalho é dedicado à minha esposa, **Maria de Fátima,** pelo incentivo, carinho e pela compreensão.

AGRADECIMENTOS

Ao meu pai, por ser exemplo de pessoa que acredita no estudo como meio de tornar a vida melhor e mais digna.

À minha mãe, por me mostrar que persistência e força de vontade são essenciais para vencer na vida.

À minha esposa, pela paciência comigo neste período de ausência, pela força nos momentos de dificuldade, incentivando sempre.

Ao Professor Leonardo, pela orientação deste trabalho, sempre pronto a ensinar, incentivando e tolerando minhas imperfeições.

À Maria de Lourdes (Lú), minha cunhada, pelo auxílio na formatação deste trabalho, sempre prestativa e dedicada a resolver os eventuais problemas do Word.

Ao Maurício Venturin, amigo e colega que foi o primeiro incentivador do assunto deste trabalho.

A Det Norske Veritas que me proporcionou a oportunidade da utilização do caso estudado neste trabalho e pelo apoio fornecido.

RESUMO

A informação tem sido apontada como a principal fonte de poder dentro das organizações e, como tal, desejada e precisa ser protegida. Para isso a Norma BS 7799 define diretrizes para implementação de um Sistema de Gerenciamento de Segurança de Informações, cujo objetivo é garantir a integridade, confidencialidade e disponibilidade da informação. O objetivo deste estudo é avaliar os resultados da aplicação de procedimentos padrões utilizados para nortear o processo de auditoria em um Sistema de Gerenciamento de Segurança de Informações, baseado na Norma BS 7799. O método utilizado foi o estudo de caso, o qual possibilitou acompanhar as etapas de um processo de certificação de um Sistema de Gerenciamento de Segurança de Informações em uma empresa no Brasil. Como principal resultado, os procedimentos que definem as diretrizes para realização do processo de auditoria, em um Sistema de Gestão da Segurança da Informação, são adequados para utilização no mercado nacional. Pequenos ajustes podem ser introduzidos nos procedimentos, a fim de facilitar as etapas de elaboração de proposta e definição da carga de auditoria.

Palavras-chave: Segurança da informação; Norma BS 7799; auditoria; auditores.

ABSTRACT

The information has become one of the main source of power within the organizations and thus, very much desired and must be protected. For this the BS 7799 standard defines requirements for the implementation of an Information Security Management System that aims at providing the integrity, confidentiality and availability of information. The objective of this study is to evaluate the results of standard procedures used to guide the audit process in an Information Security Management System based on BS 7799. The research methodology used was case study, which guided the certification process steps of an Information Security Management System into a Brazilian company. The procedures that define the requirements for the accomplishment of the audit process in an Information Security Management System can be quoted as the main results, and are adequate for using in the national market. Small adjustments can be introduced in the procedures to facilitate the stages of the proposal establishment and definition of audit time.

Key words: Information security; Standard BS 7799; audit; auditor.

SUMÁRIO

LISTA DE FIGURAS

CAPÍTULO 1

1 INTRODUÇÃO

Embora empresas reconheçam o valor da informação, é comum a geração de dados de forma abundante, onerosa, desordenada e sem uso apropriado por parte da gerência. Em geral, as organizações montam pesadas estruturas e despendem recursos para obter dados que não são analisados e que não são capazes de promover ações de melhorias, pois não se transformam em informações úteis (NASCIMENTO, 1997).

Dados são registros de fatos ou eventos que podem se transformar em informação, desde que alocados em sistemas logicamente arquitetados para medir a performance do negócio, segundo parâmetros de importância para o seu sucesso. Embora dados sejam ingredientes importantes, por si só não produzem informações relevantes e oportunas. A organização pode ter abundância de dados, mas pode ser limitada em extrair, filtrar e apresentar fatos pertinentes que supram as necessidades do tomador de decisão.

A relação entre dados e informações é bastante estreita, embora designe diferentes estados. Essa relação de proximidade e distinção é apresentada por Davis e Olson (1987): “Em síntese, os termos dados e informações com freqüência são utilizados em formas intercambiais, porém a distinção consiste no fato de que os dados elementares são a matéria prima para prover a informação.”

É importante que os responsáveis pelo desenvolvimento de sistemas de informação tenham a consciência de que dados isolados, mesmo se em quantidade razoável, não possuem significado para o tomador de decisão. Após o tratamento desses dados pelos recursos de

informática disponíveis e, seguindo critérios racionais ou intuitivos do usuário, eles poderão ser transformados em informação e disponibilizados no momento e na forma adequados para serem utilizados com eficiência pelo usuário. As necessidades de informação são diferentes para cada usuário e diferentes tomadores de decisão podem considerar diferentes informações como relevantes.

Segundo Freitas *et al*.(1997), a relação entre a organização e a informação é bastante estreita. A influência da qualidade da informação disponível na organização é grande, daí a preocupação crescente com a administração desse recurso. A atenção que os gerentes e técnicos envolvidos no processo de administração da informação devem ter com as características dos atributos da informação é fundamental para dispor de um recurso que possa contribuir para que a organização alcance seus objetivos e estratégias.

Mintzberg e Quinn (2001) apresentam cinco abordagens de estratégia: plano, manobra, padrão, posição e perspectiva. Como plano, a estratégia é um método de ação para diferentes situações, que pode ser geral ou específica. Quando a estratégia é específica, ela é vista como uma manobra que pode ter a intenção de amedrontar competidores. Como um padrão, a estratégia torna-se o próprio comportamento de uma empresa, que pode estar consciente dele ou não. A estratégia como posição identifica qual a situação da empresa no mercado, sua posição no ambiente. Como perspectiva, é a visão de mundo que a empresa tem.

Segundo Porter (1986), a estratégia é a criação de uma posição singular e valiosa, envolvendo um conjunto diferente de atividades. A essência do posicionamento estratégico é escolher atividades que sejam diferentes das atividades dos concorrentes.

Para Beuren (2000), a definição e tradução da estratégia, de forma compreensível e factível aos membros da organização, passa pela necessidade de disponibilizar informações adequadas aos responsáveis pela elaboração da estratégia empresarial. A adaptação da empresa aos novos paradigmas de um mercado global, exige capacidade de inovação, flexibilidade, rapidez, qualidade, produtividade, dentre outros requisitos, tornando cada vez mais estratégico o papel que a informação exerce.

A informação é fundamental no apoio às estratégias e processos de tomada de decisão, bem como no controle das operações empresariais. Sua utilização representa uma intervenção no processo de gestão, podendo, inclusive, provocar mudança organizacional, à

medida que afeta os diversos elementos que compõem o sistema de gestão (BEUREN, 2000). Esse recurso, quando devidamente estruturado, integra as funções das várias unidades da empresa, por meio dos diversos sistemas organizacionais.

A informação é um ativo valioso para as organizações. Por esse motivo, implementar um sistema de segurança de informações para proteger os recursos da empresa (sistemas, pessoas, informações, equipamentos, etc.) tem a finalidade de diminuir o nível de exposição aos riscos existentes em todos os ambientes, gerando assim a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. Para Moreira (2001), os negócios atualmente estão cada vez mais dependentes das tecnologias e estas por sua vez precisam proporcionar confidencialidade, integridade e disponibilidade das informações.

Quando as organizações despertam para a necessidade de uma prática ativa de segurança em seus negócios, elas começam a estendê-la aos processos, às informações, aos clientes, funcionários, produtos e serviços. Alguns dos benefícios obtidos com essa prática são:

a) riscos contra vazamento de informações confidenciais/sigilosas;

b) redução da probabilidade de fraudes;

c) diminuição de erros devido a treinamentos e mudança de comportamentos;

d) manuseio correto de informações confidenciais.

Os projetos de Segurança de Informações procuram abranger pelo menos os processos mais críticos do negócio da organização. O resultado esperado com tais projetos é que os investimentos efetuados devam conduzir para:

a) redução da probabilidade de ocorrência de incidentes de segurança;

b) redução dos danos/perdas causados por incidentes de segurança;

c) recuperação dos danos em caso de desastre/incidente.

O objetivo da segurança, no que tange à informação, é a busca da disponibilidade, confidencialidade e integridade dos seus recursos e da própria informação (MOREIRA, 2001).

A necessidade de identificar dispositivos, para gestão da segurança da informação, originou a Norma Britânica BS 7799 de Gerenciamento de Segurança de Informações. Criada em 1995, justamente com o intuito de garantir às organizações uma ferramenta que possibilita às mesmas a implementação de um sistema que possa auxiliar na garantia da disponibilidade, confidencialidade e integridade da informação, esteja esta em meio eletrônico ou não. No Brasil, as discussões sobre a utilização dessa norma como referência para implementar e manter um Sistema de Gerenciamento de Segurança de Informações iniciou a menos de dois anos, evidenciando um importante mercado latente a ser desenvolvido. Internacionalmente aplicado na empresa Det Norske Veritas (DNV), existe um modelo para definição das etapas do processo de auditoria de um Sistema de Gerenciamento de Segurança de Informações. Isso leva à necessidade de utilizar um modelo para a definição das etapas do processo de auditoria em Segurança de Informações, adequado ao mercado brasileiro, de acordo com determinações internacionais?

A relevância deste trabalho está em avaliar o atendimento ao modelo praticado mundialmente pela Det Norske Veritas – DNV e a possível demanda de segurança das informações no mercado nacional. A ausência de estudos científicos sobre como as empresas (organismos certificadores) estão tratando o assunto e quais os resultados que podem ser obtidos, a partir da implantação dessa sistemática, justificam este estudo.

1.1 OBJETIVOS

Avaliar a aplicação do modelo adotado na definição das etapas de auditoria de Sistema de Gerenciamento de Segurança de Informações, baseado na Norma BS 7799, em empresas que atuam no mercado brasileiro.

1.1.1 *Objetivos Específicos*

Os objetivos específicos do trabalho são:

a) identificar fatores críticos na utilização do modelo nas etapas dos processos de execução da auditoria de Sistema de Gerenciamento de Segurança de Informações no mercado nacional;

b) identificar facilitadores na utilização do modelo nas etapas dos processos de execução da auditoria de Sistema de Gerenciamento de Segurança de Informações no mercado nacional;

c) identificar resultados da aplicação do modelo na execução de uma auditoria em um Sistema de Gerenciamento de Segurança de Informações.

1.2 MÉTODO DE PESQUISA

O método de pesquisa utilizado neste trabalho foi o estudo de caso, que tem como uma de suas definições (YIN, 2001), "[...] tentar esclarecer uma decisão ou um conjunto de decisões: o motivo pelo qual foram tomadas, como foram implementadas e com quais resultados".

Essa definição cita o tópico das decisões como foco principal dos estudos de caso. Para Yin (2001), o estudo de caso envolve uma lógica de planejamento que segue duas maneiras. A primeira delas define o estudo de caso como uma investigação empírica que analisa um fenômeno contemporâneo dentro do seu contexto da vida real, especialmente quando os limites entre os fenômenos e o contexto não estão claramente definidos.

Em segundo lugar, uma vez que o fenômeno e contexto não são sempre discerníveis em situações da vida real, um conjunto de outras características técnicas, como a coleta de dados e as estratégias de análise de dados, torna-se a segunda parte da definição e a investigação de estudo de caso enfrenta uma situação tecnicamente única em que haverá muito mais variáveis de interesse do que pontos de dados e, como resultado, baseia-se em várias fontes de evidências, com os dados precisando convergir para estas evidências. Também pode beneficiar-se do desenvolvimento prévio de proposições teóricas para conduzir a coleta e a análise de dados.

Segundo Yin (2001), o estudo de caso, como estratégia de pesquisa, compreende um método que abrange desde a lógica de planejamento, incorporando abordagens específicas, até a coleta de dados e a análise de dados. Nesse sentido, o estudo de caso não é nem uma tática para coleta de dados nem meramente uma característica do planejamento em si, mas uma estratégia de pesquisa abrangente.

A aplicação desse método neste trabalho foi em decorrência de que o processo de auditoria em uma empresa é um fato contemporâneo, dentro do contexto de cada organização, que busca a implantação e certificação em Sistemas de Gerenciamento de Segurança de Informações, sendo esse sistema uma ferramenta interativa que constantemente sofre mudanças e utiliza essas mudanças para realimentar o próprio sistema. Logo, essas modificações constantes são decorrência de uma gama de variáveis e de diversas fontes de evidências que devem ser constatadas e verificadas em um processo de certificação do Sistema de Gerenciamento de Segurança de Informações. Assim o fato de o auditor necessitar buscar essas evidências em um ambiente contemporâneo, de constante modificação, com inúmeras variáveis a serem consideradas e baseado em uma norma que permite a elaboração de questionamentos prévios a serem verificados, conduziu a utilização do estudo de caso como método de pesquisa neste estudo. O detalhamento da utilização deste método de pesquisa está descrito no capítulo quatro.

Estudo de caso busca criar teorias gerais do conhecimento a partir do caso (ou casos) em estudo. Este trabalho avalia a utilização de procedimentos para auditoria em BS 7799, com o objetivo de avaliar se pode ser aplicado no cenário do mercado brasileiro.

1.3 LIMITAÇÕES DO TRABALHO

Destacam-se como principais limitações o fato de que o mercado nacional apresentava apenas uma opção de aplicação do modelo de auditoria, em uma empresa que possuía um Sistema de Gerenciamento de Segurança de Informações implementado. Ainda, em virtude da criticidade do assunto gerenciamento de segurança de informações, as organizações decidem por não divulgar parte dos dados utilizados para a realização de pesquisa. Também não é intenção do presente trabalho definir nenhum método de consultoria para implantação de um Sistema de Gestão de Segurança de Informações baseada na Norma BS 7799.

1.4 ORGANIZAÇÃO DO TRABALHO

A organização do presente estudo se apresenta da seguinte forma.

No capítulo 1 é apresentado o tema e a definição do objetivo geral e dos específicos; da metodologia de pesquisa e das limitações do trabalho.

No capítulo 2 trata-se da fundamentação teórica de sistemas de informação na gestão empresarial, da qualidade em sistemas de informação, do papel estratégico da segurança de informações na gestão das organizações.

No capítulo 3 são revisados os conceitos gerais sobre segurança, requisitos para a implantação de um sistema de segurança de informações com base na norma BS 7799, do estado da arte em segurança de informações, bem como a descrição do resultado de uma experiência com essa implantação.

O capítulo 4 do estudo refere-se à metodologia do estudo e a apresentação da empresa objeto desse trabalho.

No capítulo 5 são apresentados os procedimentos padrão e à análise dos dados.

Finalmente, o capítulo 6 apresenta as conclusões do estudo, considerações e sugestões para trabalhos futuros.

CAPÍTULO 2

2 SISTEMA DE INFORMAÇÃO NA GESTÃO EMPRESARIAL

Este capítulo apresenta uma visão da importância da informação para as organizações na gestão empresarial e estratégica; a influência da padronização e qualidade como fator de confiabilidade para as organizações; o papel estratégico da segurança da informação nas organizações.

2.1 GESTÃO EMPRESARIAL E ESTRATÉGICA

A influência da tecnologia na sociedade moderna é intensa, principalmente no que se refere à tecnologia da informação. A velocidade com que a tecnologia da informação evolui tem reflexos diretos na sociedade que a utiliza. Murdick e Munson (1988), citam alguns fatores que repercutem diretamente na sociedade e nas empresas:

a) o aumento do conhecimento em computação entre os líderes e a população em geral;

b) o aprimoramento nas telecomunicações (fibras óticas, satélites, redes e bases de dados) em nível internacional;

c) o surgimento, a transformação e a proliferação dos microcomputadores;

d) a conexão de microcomputadores das empresas a computadores de grande porte, utilizando grandes bases de dados;

e) a utilização de *lasers* para registrar informações em discos;

f) a interação do ser humano com o computador, utilizando voz; os chips utilizados na computação, etc.

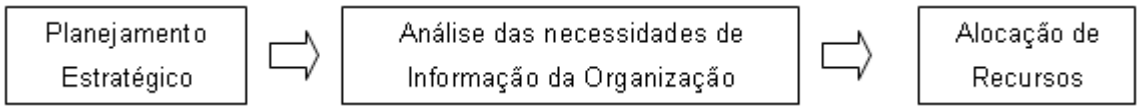
À medida que as organizações crescem e se tornam mais complexas, ocorre um aumento da necessidade e da importância da informação. A informação passa a ser não somente útil em nível operacional, mas também em níveis tático e estratégico. Nesse contexto, não apenas o conteúdo da informação é relevante, mas a forma como a informação é trabalhada ganha importância. A eficácia no tratamento da informação depende, em grande parte, de como ela é administrada e do bom entendimento de certos conceitos e relações, sob pena de se fornecer ao usuário apenas dados desconexos, comprometendo o processo decisório.

A informação, como um precioso recurso para a organização, deve ser tratada de modo a contribuir efetivamente para a melhoria dos resultados organizacionais. A organização necessita identificar onde encontrar as informações relevantes para o seu processo. Essa informação pode ser conseguida em fontes formais e informais. As fontes informais (fofocas, rádio-corredor, conversas, feiras, congressos, imprensa), e que não possuem caráter oficial, têm como característica serem desestruturadas e dificilmente serão incluídas em um Sistema de Informações. As fontes formais, que normalmente tramitam pelos canais convencionais da organização, têm a característica de ser estruturadas e podem ser tanto de origem interna como externa e assim mais facilmente integrar o Sistema de Informações da organização e isso dependerá exclusivamente da análise de custo/beneficio. Já as necessidades de informações variam de acordo com o nível organizacional em que a decisão ocorre. As informações fornecidas por um Sistema de Informação devem atender a alguns atributos essenciais (características importantes tais como finalidade, modo e formato, redundância e eficiência, velocidade e outros), para que possam ser significativas no momento da tomada de decisão. É necessário que a informação seja relevante para a situação, pois de nada adianta à informação possuir todos os atributos desejados, se não for pertinente à situação que o decisor está enfrentando.

A competitividade do mercado está constantemente exigindo dos competidores respostas rápidas e eficientes. A informação é um importante fator de diferenciação. Segundo Bio (1988), é necessário que a organização construa um Sistema de Informações, subsidiando

o processo de tomada de decisão para, dessa forma, contribuir para um melhor desenvolvimento do processo decisório.

A política de informação existente na organização vai influenciar as características dos sistemas de informação utilizados pelos gerentes e deve estar de acordo com a estratégia geral da organização. Deve haver sincronismo entre o planejamento estratégico da organização e sua política de informação. A organização, principalmente os responsáveis pelas suas decisões estratégicas, deve pensar na informação como um de seus mais importantes componentes. Furlan (1991), comenta que o planejamento estratégico dos sistemas de informação deve estar contido no próprio planejamento estratégico da organização. A visão do autor corrobora o modelo de planejamento de sistemas indicado por Kugler e Fernandes (1984), que prevê que a análise das necessidades de informação da organização decorre do planejamento estratégico para posterior alocação de recursos, conforme demonstra a Figura 1.



Fonte: adaptado de Kugler e Fernandes (1984)
Figura 1 Estágios para o planejamento de sistemas

Nas organizações, a informação já é considerada como um recurso básico e essencial, como o são a mão-de-obra e a matéria-prima. A informação é vista como um elemento decisivo, que pode determinar o êxito ou o fracasso de um empreendimento. Kendall e Kendall (1999), comentam que “os responsáveis pela tomada de decisão começam a considerar que a informação já não é um produto exclusivamente colateral das operações da empresa, e sim, um dos promotores da mesma”. Tofler (1985), acredita que a informação é até mais importante do que os fatores trabalho, capital e matéria-prima. Freitas (1992) comenta que o tratamento da informação pela organização pode ser categorizado como a “função informacional da empresa” e acredita que “este processo é cada vez mais vital para a empresa e deve ser controlado como todos os outros setores”.

As organizações estão inseridas em um mercado instável e competitivo, onde as ameaças e oportunidades aparecem muito rapidamente. Segundo Porter (1992), cinco forças básicas influenciam a competitividade da empresa:

a) concorrência dentro da indústria;

b) ameaça de novos entrantes no mercado;

c) poder de negociação dos compradores;

d) poder de negociação dos fornecedores e

e) ameaça de produtos e serviços substitutos.

Nessa perspectiva, a informação pode ser usada no sentido de identificar alternativas para provocar mudanças no poder de barganha da empresa com o ambiente externo, para remover ou criar barreiras à entrada de novos concorrentes, para diferenciar uma empresa das demais que atuam no mesmo segmento, para configurar novas cadeias de valor, para penetrar em economias diferenciadas.

Para auxiliar as organizações a sobreviver e prosperar nesse ambiente, a informação é um dos elementos cruciais e, para isso, elas precisam ter como suporte uma adequada tecnologia da informação. Para Porter e Millar (1985), a tecnologia da informação se caracteriza como uma vantagem competitiva, tanto no que se refere ao custo, quanto no que se refere à diferenciação dos produtos ou serviços.

Já para Beuren (2000), o uso estratégico da informação resulta em vantagem competitiva se ele contribuir, efetivamente, na identificação de alternativas que aperfeiçoam o desempenho da organização em todos os níveis, lançando-a, inclusive, à liderança no segmento em que atua. Dessa forma, a empresa pode alterar as regras da competição por meio da mudança de seus processos. Ainda, segundo Beuren (2000), existem várias formas para as empresas obterem vantagens competitivas por intermédio do uso da informação. Uma delas implica realizar investimentos em informação e tecnologia da informação. Ambas são recursos importantes para a formulação da estratégia, especialmente no que diz respeito ao resgate da memória organizacional relacionada a clientes, fornecedores, concorrentes, velocidade para viabilizar tecnicamente um programa de atendimento a clientes internos e externos, avaliação de desempenho de estratégias definidas em momentos anteriores.

Outro uso estratégico da informação implica embuti-la em produtos e serviços já existentes na empresa. Em vários segmentos de negócio, o sucesso da organização, dependerá da sua capacidade de identificar e satisfazer às necessidades de seus clientes, associando ou dissociando a informação aos produtos ou serviços por ela comercializados, e ainda, uma

outra maneira de usar a informação para criar vantagem competitiva, segundo Beuren (2000), é a aprendizagem organizacional que a empresa adquire acumulando informações e aprendendo sobre os diferentes usos destas informações, o que aumenta sua capacidade de impor barreiras de entrada entre segmentos de negócios, ou seja, mais difícil se torna a supremacia dos concorrentes nessa estratégia.

Também na prestação de serviços, segundo Fitzsimmons e Fitzsimmons (2000), a informação é a tecnologia habilitadora dos processos de inovação. A função estratégica da informação em serviços é organizada em quatro categorias: criação de barreiras à entrada, geração de renda, vantagens pelo uso de banco de dados e intensificação da produtividade conforme se pode observar na Figura 2.

O gerenciamento de rendimento, lançado pela *American Airlines*, é o mais abrangente uso da informação para fins estratégicos e a melhor ilustração da natureza integrada dos serviços para Fitzsimmons e Fitzsimmons (2000). Utilizando métodos de previsão de demanda, vindos do gerenciamento de operações; estratégias de preços, vindas do marketing, e a psicologia do consumidor, vinda do comportamento organizacional, a *American Airlines* desenvolveu um método computacional para vender passagens aéreas a preços variados, a fim de maximizar a renda em qualquer vôo. O conceito de uma cadeia de valor virtual propicia uma visão da inovação em serviços, que cria valor utilizando a informação coletada enquanto o cliente é atendido.

Uso Competitivo da Informação

Focalização Estratégica	*On-line* (em tempo real)	*Off-line* (análise)
Externa (cliente)	Criação de barreiras à entrada de competidores, exemplos: Sistemas de reservas Clube do usuário freqüente Transferência de custos	Vantagens por uso de banco de dados exemplos: Venda de informações Desenvolvimento dos serviços Micromarketing
Interna (operações)	Geração de renda, exemplos: Gerenciamento da renda Ponto de vendas Sistemas especialistas	Intensificação da produtividade exemplos: Situação dos estoques Análise por envelopamento de dados

Fonte: adaptado de Fitzsimmons e Fitzsimmons (2000)

Figura 2 Funções estratégicas da informação em serviços

Ainda para reforçar a importância da informação para as organizações, Laudon e Laudon (1999) comentam que, embora qualquer aplicação de um sistema de informações seja importante no sentido de que ele resolve algum problema empresarial importante, um sistema estratégico de informações é aquele que proporciona vantagem competitiva. Os sistemas de informações têm uma ação de grande alcance e estão arraigados, possibilitando a mudança dos objetivos, produtos, serviços ou das relações internas e externas da empresa.

Entretanto, nem todos os executivos estão conscientes dessa importância. Mendes (1987), aponta que os altos executivos das empresas brasileiras não participam das definições estratégicas relacionadas à tecnologia da informação. Um dos motivos para o baixo envolvimento desses executivos foi a utilização não muito satisfatória da informática, sendo empregada basicamente para auxiliar atividades burocráticas. Pesquisa de Kini (1993), mostra que, “embora 97% dos gerentes das áreas de informática acreditem que a tecnologia da informação pode gerar vantagem competitiva, apenas 19% institucionalizaram tais sistemas”.

Oliveira e Grajew (1987), concordam com essa crítica em relação à informática, porém acreditam que esse quadro esteja mudando, principalmente com relação à utilização dos recursos de informática como ferramenta competitiva.

A competitividade do mercado está sempre exigindo dos competidores respostas rápidas e eficientes. A informação é um importante fator de diferenciação e deve ser usada como vantagem competitiva.

Apesar dos problemas relacionados com a tecnologia da informação e utilização dos recursos da informática, a importância competitiva da informação é consenso. Para Davenport *et al.* (1992), os executivos já perceberam essa importância, pois, “durante a década de 90, as organizações entenderam que a informação é um de seus mais críticos recursos, sendo que o grande acesso, a utilização e o aumento de sua qualidade são fatores chave para aumentar a performance do negócio”. Essa opinião é compartilhada por Watson *et al.* (1997), acrescentando que os administradores de sistemas de informações estão se preocupando principalmente com a utilização da informação em questões estratégicas. Kini (1993), salienta que as informações utilizadas em questões estratégicas podem fornecer vantagem competitiva às organizações.

Porter e Millar (1985), retratam a questão da informação como fator de competitividade:

> "A importância da revolução da informação não está em discussão. A questão não é se a tecnologia da informação vai ter um impacto significante na posição competitiva da empresa. A questão é quando e como o impacto vai acontecer. Empresas que se preparam com o poder da tecnologia da informação estarão no controle dos eventos. Empresas que não se prepararem serão forçadas a aceitar as mudanças que os outros iniciaram e estarão em desvantagem competitiva".

A empresa contemporânea fabrica secundariamente informação, mas para que se traduza realmente numa ferramenta para a gestão, é necessário que seja apresentada por sistemas de informação com a qualidade adequada para o atendimento aos requisitos definidos por quem irá utilizá-la.

2.2 PADRONIZAÇÃO E QUALIDADE EM SISTEMAS DE INFORMAÇÃO

A definição de qualidade em sistemas de informação é, basicamente, sistemas que funcionam sem defeitos, apresentando uma imagem de confiabilidade para seus usuários (TAURION, 1996). Em sistemas de informação, a garantia de qualidade é incipiente, sendo que, na maioria das organizações, os processos de testes são ainda rudimentares e ineficientes, muitas vezes realizados manualmente, sem o apoio de processos e softwares especializados. É ainda comum que programadores sejam os únicos responsáveis pelos testes (e garantia da qualidade) dos programas que eles mesmos desenvolvem. Ignora-se o fato de que dificilmente uma pessoa encontra todos os seus possíveis erros no seu próprio processo de desenvolvimento de programas.

O movimento de qualidade, observado nas empresas brasileiras a partir de 1980, chegou também às empresas ligadas ao setor de tecnologia da informação, inicialmente nas empresas de *hardware*, e, nos últimos dez anos, também nas empresas de *software* (TAURION, 1996). Um dos motivos para tal movimento foi a exigência, por parte de consumidores, especialmente os industriais, de fornecedores capazes de projetar, desenvolver e entregar produtos que atendessem aos seus requisitos. Apesar da exigência do mercado por qualidade, as ações da maioria dos fornecedores no sentido de alcançá-la ainda são incipientes. Implementar qualidade de *software* exige uma mudança na própria cultura da organização (TAURION, 1996). Nesse sentido, buscar um nível adequado de maturidade

organizacional e tecnológica é fundamental para que uma abordagem voltada para a qualidade tenha sucesso.

Especificamente em relação ao processo realizado pela organização, para desenvolver sistemas, pode-se destacar a noção de maturidade organizacional. Segundo Taurion (1996), cerca de 50% do custo de um projeto estão relacionados com atividades de teste. Entretanto, o custo do não-teste (ou não qualidade) pode ser ainda superior, gerando insatisfação do cliente, decorrente da instabilidade além da falta de confiabilidade no sistema.

Sem um processo formal de testes, suportado por ferramentas especializadas, dificilmente serão produzidas aplicações com baixo índice de defeitos. Uma aplicação de missão crítica defeituosa, além de prejuízos financeiros, pode colocar em risco a organização que a utiliza. Segundo Humphrey (1997), citado por Weber *et al*. (2000), para que a indústria de software contribua de forma construtiva para a sociedade, precisa-se aprender a entregar produtos com qualidade, no prazo estabelecido e com custos planejados. Isto não é impossível. Outras indústrias, à medida que amadureceram, atingiram este nível de desempenho. Não há razão para que isto não seja possível para *software*.

Partindo de afirmações como essa, foram elaboradas normas (NBR ISO/IEC 12207, normas da série ISO 9000, *Capability Maturity Model* - CMM, *Control Objectives for Information and Related Technology* – COBit – e outras), que procuram estabelecer abordagens para melhorias no processos e na tomada de decisão, sendo necessário uma sistemática estruturada para gerenciar e controlar as iniciativas de tecnologia da informação nas empresas, para garantir o retorno de investimentos e adição de melhorias nos processos empresariais.

Também em termos específicos as normas podem contribuir para a melhoria da qualidade dos processos de *software* e têm como objetivo principal estabelecer uma estrutura comum de processos de *software*, que seja utilizada como referência na contratação de produtos e serviços desse gênero, bem como descrever as melhores práticas de engenharia e gerenciamento de *software*.

A estrutura das normas é composta de processos, atividades e tarefas, a serem aplicados em operações que envolvam o *software* de alguma forma, seja na aquisição, no fornecimento, desenvolvimento, na operação ou manutenção. Essa estrutura também permite

estabelecer ligações claras com o ambiente da engenharia de sistemas, ou seja, aquele que inclui *software*, *hardware*, pessoal e práticas de negócios.

A Norma ISO/IEC 12207 agrupa os processos do ciclo de vida do *software* em três classes: processos fundamentais, processos de apoio e processos organizacionais. Cada processo é definido em termos de suas próprias atividades, e cada atividade é definida em termos de suas tarefas. Uma tarefa é expressa pelo verbo que a descreve: um requisito (deve), uma declaração de objetivos ou intenção (deverá), uma recomendação (deveria) ou uma ação permissível (pode) (MOREIRA, 2001).

Processos fundamentais: são aqueles que atendem ao início e à execução do desenvolvimento, da operação ou manutenção de produtos de software, segundo Weber *et al.* (2001). Durante o ciclo de vida do software os processos fundamentais são:

a) **processo de aquisição:** define as atividades do adquirente, organização que adquire um sistema ou produto de *software*;

b) **processo de fornecimento:** define as atividades do fornecedor, organização que provê o produto de software ao adquirente;

c) **processo de desenvolvimento:** define as atividades do desenvolvedor, organização que define e desenvolve o produto de *software*;

d) **processo de operação:** define as atividades do operador, organização que provê serviço de operação de um sistema computacional no seu ambiente de funcionamento para seus usuários;

e) **processo de manutenção:** define as atividades do mantenedor, organização que provê os serviços de manutenção do *software*, isto é, o gerenciamento de modificações no *software*, a fim de mantê-lo constantemente atualizado e em perfeita operação.

Processos de apoio: são aqueles que auxiliam e contribuem para o sucesso e a qualidade do projeto de *software*. Um processo de apoio é empregado e executado, quando necessário, por outro processo, e são:

a) **processo de documentação:** define as atividades para registrar informações produzidas por um processo ou atividade do ciclo de vida;

b) **processo de gerência de configuração:** define as atividades para a aplicação de procedimentos administrativos e técnicos, por todo o ciclo de vida do *software*;

c) **processo de garantia da qualidade:** define as atividades para fornecer a garantia adequada de que os processos e produtos de *software*, no ciclo de vida do projeto, estejam em conformidade com seus requisitos especificados e sejam aderentes aos planos estabelecidos;

d) **processo de verificação:** define as atividades para verificação dos produtos de *software*. É um processo para determinar se os produtos de software de uma atividade atendem completamente aos requisitos ou às condições impostas a eles;

e) **processo de validação:** define as atividades para validação dos produtos produzidos pelo projeto de *software*. É um processo para determinar se os requisitos e o produto final atendem ao uso especifico;

f) **processo de revisão conjunta:** define atividades para avaliar a situação e o produto de um projeto, se apropriado;

g) **processo de auditoria:** define as atividades para determinar adequação aos requisitos, planos e ao contrato, quando apropriado;

h) **processo de resolução de problema:** define um processo para analisar e resolver os problemas (incluindo não conformidades), de qualquer natureza ou fonte, que são descobertos durante a execução do desenvolvimento, da operação, manutenção ou de outros processos.

Processos organizacionais: são empregados por uma organização para estabelecer e implementar uma estrutura constituída de processos de ciclo de vida e pessoal associado, melhorando continuamente a estrutura e os processos. São eles:

a) **processo de gerência:** define as atividades genéricas que podem ser empregadas por quaisquer das partes que têm que gerenciar seu respectivo processo;

b) **processo de infra-estrutura:** define as atividades para estabelecer e manter a infra-estrutura necessária para qualquer outro processo;

c) **processo de melhoria:** define as atividades básicas que uma organização executa para estabelecer, avaliar, medir, controlar e melhorar um processo do ciclo de vida do *software*;

d) **processo de treinamento**: define as atividades para prover e manter pessoal treinado. A aquisição, o fornecimento, o desenvolvimento, a operação ou a manutenção de produtos de *software* são extremamente dependentes de pessoal com conhecimento e qualificação.

Basear esse ciclo de vida na Norma ISO 12207 exige, como todo o processo de implantação, uma adaptação. Este também pode ser considerado um processo que exige a definição das atividades necessárias para executar a implementação da norma na organização ou em projetos. A adaptação pode ser facilitada se for conduzida com base em fatores que diferenciam uma organização ou um projeto de outros, dentre os quais, a estratégia de aquisição, modelos de ciclo de vida de projeto, características de sistemas e software e cultura organizacional. A existência desse processo permite que a norma seja adaptável a qualquer projeto, organização, modelo de ciclo de vida, cultura e técnica de desenvolvimento cita Weber *et al.* (2001).

Outro modelo que pode ser utilizado para garantir que um sistema seja implementado com qualidade do produto/serviço é a série de Normas ISO 9000 (1994), que foi criada para padronizar os requisitos de garantia da qualidade a serem atendidos por um fornecedor e, com isso, a padronização dos programas de qualificação de fornecedores dos grandes compradores. Diante de tais benefícios, com o impulso da globalização da produção e a formação de blocos de mercados consumidores, rapidamente o modelo ISO 9000 ganhou a adesão da comunidade internacional.

A família ISO 9000 (1994) é composta de uma série de normas, mas somente as Normas ISO 9001, 9002 e 9003 podem ser utilizadas como requisitos entre clientes e fornecedores. As outras normas destinam-se a orientar a escolha da norma a ser utilizada ou à sua implantação. A ISO 9003 cobre exclusivamente as atividades de inspeção e ensaio final; a ISO 9002, as atividades de produção e serviços associados e a ISO 9001, todo o ciclo de vida de um produto ou serviço, iniciando no seu projeto ou desenvolvimento, passando pelas atividades de produção e serviços associados.

A ISO (*International Organization for Standartization*) reconhece que existem quatro diferentes categorias genéricas de produtos e publicou diretrizes para implementação de sistemas da qualidade para cada uma dessas categorias:

a) Produtos (*hardware*): ISO 9004-1;

b) Serviços: ISO 9004-2;

c) Materiais processados: ISO 9004-3; e

d) *Software*: ISO 9000-3.

Devido às dificuldades específicas de interpretação, tais como a terminologia utilizada na norma, para implantação dos requisitos da ISO 9001 ou ISO 9002 em software, o uso da ISO 9000-3 para auxiliar a implantação do sistema de gestão da qualidade torna-se fundamental.

A certificação ISO 9000 é reconhecida em praticamente todos os países e setores, não só pelo setor de *software*. Para uma empresa, conquistar a certificação ISO 9000 significa alcançar padrão internacional de qualidade em seus processos de *software*. Entretanto, mesmo no âmbito de um determinado setor, não é possível diferenciar o nível de maturidade de uma empresa em relação à outra. Em um conjunto de empresas de *software*, no qual todas tenham recebido certificação ISO 9000, a diferenciação só pode ser feita pelo escopo da certificação, pela credibilidade do organismo certificador e pelo tempo que a certificação vem sendo mantida.

Em 2000, a série de Normas ISO 9000 sofreu uma revisão, onde a principal modificação em relação à anterior foi a mudança do objetivo principal da Norma, anteriormente denominada “Sistema de Garantia da Qualidade”, que visava atender aos requisitos especificados do cliente, para “Sistema de Gestão da Qualidade” um modelo que visa alcançar a satisfação desse cliente. Dessa forma, deixou de ser um modelo que visa exclusivamente garantir o atendimento às especificações estabelecidas, para ser um modelo que visa à criação de um sistema de gestão da qualidade mais abrangente e que tem como fim a satisfação do cliente. Essa satisfação está relacionada principalmente com a percepção da qualidade dos produtos e serviços fornecidos, o que envolve não apenas os requisitos especificados, explícitos (por ex.: a escolha da cor de um eletrodoméstico), mas também requisitos implícitos (por ex.: a sua voltagem). Em conseqüência, a estrutura da família de Normas ISO 9000:2000 também foi modificada: as Normas ISO 9002 e ISO 9003 deixaram de existir, e a ISO 9001:2000 permitirá que se façam exclusões de requisitos contidos no item 7 – Realização de produto (NBR ISO 9001:2000).

Outro exemplo de padronização, que pode auxiliar a organização a obter melhor desempenho, é o *Capability Maturity Model* - CMM. O modelo foi desenvolvido pelo *Software Engineering Institute* (SEI), sendo financiado pelo departamento de Defesa Americano, com o objetivo de estabelecer um padrão de qualidade para software desenvolvido para as Forças Armadas. O CMM foi concebido para o desenvolvimento de grandes projetos militares e, para sua aplicação em projetos menores e em outras áreas. Foi baseado nos conceitos de Qualidade Total estabelecidos por Crosby (MOREIRA, 2001), que mostrou que a implantação de sistemas da qualidade em empresas segue um amadurecimento gradativo, em patamares que denominou: incerteza, despertar, esclarecimento, sabedoria e certeza.

No modelo CMM foram estabelecidos níveis referentes à maturidade que a organização possui para desenvolver *software*: inicial, repetível, definido, gerenciado e otimizado. Cada nível de maturidade está dividido em áreas-chave de processo, que estabelecem grandes temas a serem abordados, totalizando dezoito áreas-chave. Cada uma dessas áreas é detalhada nas práticas-chave, que traduzem os quesitos a serem cumpridos na implantação do modelo. Como todo modelo, as práticas-chave especificam “o quê” deve ser cumprido, exigindo documentos, treinamentos ou definição de políticas para as atividades, mas nunca especificam “como” elas devem ser implementadas.

Cabe considerar que o CMM é apenas um modelo que reúne boas práticas de desenvolvimento de *software*. Sua implantação vai exigir um investimento importante dos envolvidos, para conceber um processo que venha a alavancar o negócio, facilitar a vida dos envolvidos e não criar burocracia somente para atender aos requisitos descritos no modelo, conforme citam Weber *et al*. (2001).

E ainda um último exemplo de modelo é o *Control objectives for information and related technology* - Cobit, que é um guia para a gestão de tecnologia da informação recomendado pelo *Information Systems Audit and Control Foundation* (ISACF). O Cobit inclui recursos tais como um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento.

Segundo Fagundes (2004) as práticas de gestão do Cobit são recomendadas pelos peritos em gestão de tecnologia da informação que ajudam a otimizar os investimentos de

tecnologia da informação e fornecem métricas para avaliação dos resultados. O Cobit independe das plataformas de tecnologia da informação adotadas nas empresas.

O Cobit, fornece informações detalhadas para gerenciar processos baseados em objetivos de negócios. O Cobit é projetado para auxiliar três aspectos distintos, conforme cita Fagundes (2004):

a) gerentes que necessitam avaliar o risco e controlar os investimentos de tecnologia da informação em uma organização;

b) usuários que precisam ter garantias de que os serviços de tecnologia da informação que dependem os seus produtos e serviços para os clientes internos e externos estão sendo bem gerenciados;

c) auditores que podem se apoiar nas recomendações do Cobit para avaliar o nível da gestão de tecnologia da informação e aconselhar o controle interno da organização.

O Cobit está dividido em quatro domínios:

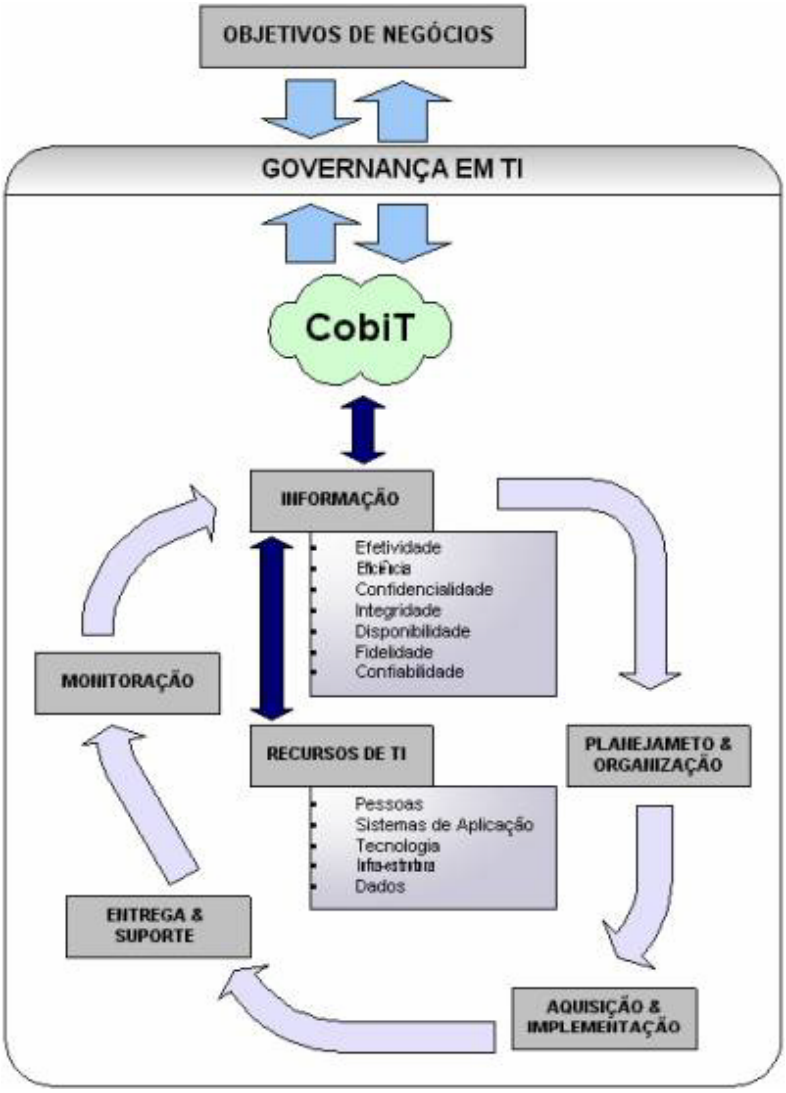
a) planejamento e organização;

b) aquisição e implementação;

c) entrega e suporte;

d) monitoração.

A Figura 3 ilustra a estrutura do Cobit com os quatro domínios, onde claramente está ligado aos processos de negócio da organização. Os mapas de controle fornecidos pelo Cobit auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de tecnologia da informação e recomendar a implementação de novas práticas, se necessário. O ponto central é o gerenciamento da informação com os recursos de tecnologia da informação para garantir o negócio da organização.



Fonte: Fagundes (2004)

Figura 3 Estrutura do Cobit

2.3 SEGURANÇA DE INFORMAÇÕES NA GESTÃO EMPRESARIAL

Caruso *et al*. (1999) citam que o bem mais valioso de uma empresa pode não ser aquele produzido na sua linha de produção ou estar no serviço prestado, mas são as informações relacionadas a esse bem de consumo ou serviço. Ao longo da História, o homem buscou o controle das informações que lhe eram importantes de alguma forma. O que mudou desde então foram as formas de registro e armazenamento das informações. Na Pré-História e até mesmo nos primeiros milênios da Idade Antiga, o principal meio de armazenamento e registro de informações era a memória humana. Com o advento dos primeiros alfabetos, isso

começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações.

Nesse contexto, com uma tecnologia incipiente e materiais pouco apropriados para o registro de informações, o controle e a disseminação da tecnologia relacionada com as informações estavam restritos a uma minoria sempre ligada ao grupo que dominava o poder econômico e político da sociedade. Os primeiros suportes para registro de informações foram as paredes das habitações humanas implicando um conjunto de conseqüências: restrições de acesso físico, de transferência para terceiros ou para outro local e de pessoal capacitado. Além da imobilidade das informações em si, o fato de a tecnologia ser de conhecimento de poucos implicava também que as mesmas estavam em código irreconhecível para os demais.

Com as mudanças tecnológicas nos meios de registro (as placas de barro dos sumérios, o papiro dos egípcios e o pergaminho), as informações passaram para meios de registro portáveis. Foi com a disseminação da tecnologia de impressão e com a alfabetização mais ampla, já no final da Idade Média, que as informações deixaram de ser códigos incompreensíveis. Apenas nos últimos dois séculos a alfabetização se popularizou nos grandes segmentos da população de diversos países, e, em meados do século XX, a alfabetização se universalizou, apesar de ainda existir parte da humanidade analfabeta.

Na atualidade, as organizações estão dependentes da tecnologia de informações, em maior ou menor grau, especialmente em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação.

Independentemente do setor da economia em que a empresa atue, as informações estão relacionadas com seus processos de produção e de negócios; com políticas estratégicas, de marketing; com cadastros de clientes, etc. Não importa o meio físico em que as informações residam, elas são de valor inestimável não só para a empresa que as gerou como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas com atividades diárias da empresa e que, sem elas, poderiam ser comprometidas.

As empresas dedicam atenção especial à proteção de seus ativos físicos e financeiros, evitando dar atenção aos ativos de informação que possuem. Da mesma forma que seus ativos

tangíveis, para as informações são considerados três fatores de produção tradicionais: capital, mão-de-obra e processos. Sendo assim, mesmo que as informações não recebam o mesmo tratamento físico-contábil que os outros ativos, do ponto de vista do negócio, elas são um ativo da empresa e, portanto, devem ser protegidas.

É importante reforçar que empresas podem não sobreviver a um colapso do fluxo de informações, não importando o meio de armazenamento das mesmas. Dada a característica de tais empreendimentos, como por exemplo serviços bancários que se caracterizam como uma relação de confiança, é fácil prever que isso acarretaria completo descontrole sobre os negócios. Os riscos são agravados em progressão geométrica à medida que informações essenciais ao gerenciamento dos negócios são centralizadas. Ainda que esses riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob os aspectos econômicos quanto sob aspectos de agilização de processos e de tomadas de decisão em todos os níveis. Essa agilidade é tanto mais necessária quanto maior for o uso de facilidades de processamento de informações pelos concorrentes.

É necessário cercar o ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável, visto ser impossível obter-se segurança absoluta, já que, a partir de determinado nível, os custos envolvidos com segurança tornam-se cada vez mais onerosos, superando os benefícios obtidos.

Segurança, mais que estrutura hierárquica, homens e equipamentos, envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas. Devido ao caráter altamente dinâmico que as atividades relacionadas com o processamento de informações adquiriram ao longo do tempo, uma política de segurança de informações deve ser o mais ampla e mais simples possível. Sendo assim, entende-se por política de segurança uma política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras claras e simples e com estrutura gerencial e material de suporte a essa política claramente sustentada pela alta administração.

É necessário delinear uma estrutura geral que não sofra as conseqüências das rápidas mutações que, freqüentemente, ocorrem com as atividades de processamento de informações. A política geral de segurança deve esboçar as regras básicas aplicáveis a toda a organização, deixando que cada área defina as regras mais detalhadas que se relacionem a atividades específicas.

Os tópicos desenvolvidos neste capítulo sintetizam o relato sobre a informação, seu papel estratégico para as organizações e a necessidade de um gerenciamento sistematizado sobre a segurança de tais informações. Organizações internacionais definiram normas para viabilizar tal sistematização, uma delas é a norma BS 7799, cujo detalhamento é apresentado no capítulo 3.

CAPÍTULO 3

3 SEGURANÇA NAS INFORMAÇÕES

O objetivo deste capítulo é definir conceitos gerais sobre segurança, dentro de uma retrospectiva histórica e definir as bases e requisitos que levaram ao surgimento da Norma BS 7799, para a implantação de um sistema de gerenciamento de segurança de informações.

3.1 CONCEITOS GERAIS SOBRE A SEGURANÇA

Ao longo da História da humanidade, sempre existiu, em maior ou menor grau, algum tipo de preocupação com a segurança de informações, mesmo que não houvesse uma forma prática e fácil de separar o acesso lógico do acesso ao suporte físico das informações propriamente ditas.

Como o meio de registro e suporte das informações era diretamente entendível, não havia um conceito preciso de acesso lógico. Isso surgiu em decorrência do desenvolvimento de sistemas de aplicações que acessam informações computadorizadas em tempo real e da proliferação dos ambientes de informática baseados em microcomputadores. Em decorrência disso, a concentração em único lugar, e o grande volume de informações passou a ser um problema sério para a segurança. Os riscos agravaram-se após o aparecimento dos microcomputadores, das redes e da Internet, bem como da disseminação da cultura de informática em segmentos expressivos da sociedade.

As organizações tornam-se dependentes de informações armazenadas em computadores, aproveitam-se da grande velocidade e capacidade de cruzamento de informações que os computadores oferecem, para obterem benefícios como rápidas tomadas de decisão, mudança rápida de estratégia e/ou tática, entre outras. (CARUSO *et al*., 1999). Mas a mesma facilidade proporcionada pelos computadores também implica alto risco de violação. O mesmo programa usado para emitir um relatório de projeção de vendas, destinado ao diretor de marketing, pode ser usado por um "espião" para emiti-lo para o diretor de marketing do concorrente.

Nem todos os riscos relacionados com o processamento de informações surgiram com o advento dos computadores. Entretanto, estes contribuíram sobremaneira para o seu agravamento. Esses riscos são decorrentes principalmente de fatores que, em maior ou menor grau, aparecem em todas as organizações, de forma geral independem do tipo e tamanho dos equipamentos. A principal diferença reside na escala e no grau de acesso existente (CARUSO *et al*.,1999).

A segurança de acesso lógico refere-se ao acesso que indivíduos têm a aplicações residentes em ambientes informatizados, não importando o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são, em sua maior parte, invisíveis aos olhos de pessoas externas aos ambientes de informática, pois estas somente reconhecem tais controles quando têm seu acesso barrado pelos mesmos.

A expressão "acesso lógico", ainda que de uso geral por profissionais da informática, não exprime o conceito envolvido, que é o acesso ao ambiente de informações. No caso de acesso físico, o objeto sujeito ao controle é tangível e o conceito é fácil de ser entendido. Por exemplo, em determinada área somente podem entrar pessoas que trabalham na mesma ou cujas funções as obriguem a ter contato com outras que ali trabalhem, ou pessoas de nível hierárquico superior, relacionadas de forma mais direta com as atividades executadas na área sob controle. Já com relação ao "acesso lógico", o objeto da verificação é invisível aos meios normais de controle, envolvendo recursos de acesso associados a indivíduos que somente são passíveis de monitoramento por meio de recursos também invisíveis aos meios normais de controle.

"Acesso lógico" está relacionado com o acesso ao conteúdo informacional. Faz mais sentido para acesso a ambientes informatizados, que são colocados à disposição de pessoas

para que executem as tarefas para as quais foram contratadas. Abrange aspectos como o acesso de pessoas a terminais e outros equipamentos de computação e manuseio de listagens, funções autorizadas dentro do ambiente informatizado, a exemplo de transações que podem ser efetuadas, arquivos aos quais tenham acesso, programas que possam executar, entre outros.

O conceito de propriedade deriva do direito de posse direta ou delegada sobre os ativos de informações, exercido em nome da empresa. Em princípio, a propriedade de um ativo pertence a quem dele faz uso em função de necessidade funcional. Normalmente, quem faz uso de determinado ativo é o seu criador, ou pessoa que recebeu autorização do mesmo. A propriedade também recebe o nome gestão, sendo que o responsável pela administração da informação é chamado de gestor.

No passado, em virtude da concentração de informações na área de informática, a mesma se considerava proprietária dos ativos de informações da companhia. Atualmente, essa tendência diminuiu, os usuários finais passaram a exercer funções originalmente centralizadas na área de informática diretamente relacionada, e até mesmo funções relacionadas com o desenvolvimento de aplicações específicas para o atendimento de suas necessidades. O usuário final tem o direito de propriedade inclusive sobre o *software* aplicativo desenvolvido pela área de informática para seu uso.

O conceito de custódia refere-se à pessoa ou à organização responsável pela guarda de um ativo de propriedade de terceiros. O mesmo conceito pode ser aplicado para informações, significando pessoa ou função, dentro da companhia, responsável pela guarda de ativos de outras pessoas ou funções. A área de informática, ao contrário da visão clássica ainda bastante aceita, é custodiante dos ativos de informações das áreas usuárias. Ela os guarda e processa em nome de seus legítimos proprietários, as áreas usuárias, para os quais os sistemas de aplicação foram desenvolvidos ou em nome dos quais são guardados. Isso vale até mesmo quando o meio de suporte é outro que não o informatizado. A custódia implica a responsabilidade do receptor quanto à integridade dos ativos custodiados. Normalmente, com a custódia, o custodiante recebe o direito de efetuar operações com os ativos custodiados em nome do proprietário, para executar serviços tanto para o mesmo como para terceiros autorizados por ele.

O controle de acesso está relacionado diretamente ao acesso concedido. A função desse controle é garantir que o acesso seja feito somente dentro dos limites estabelecidos. Esse controle é exercido por meio de mecanismos diversos:

a) **senhas:** constituem o mecanismo de controle de acesso mais antigo usado pelo homem para impedir acessos não autorizados, sendo formadas normalmente pela combinação de letras e números. São muito usadas como forma de se controlar o acesso a recursos de informação, e os métodos de controle de acesso mais recentes tendem a usar senhas como mecanismos de autenticação de identidade de usuários pela atribuição de uma senha exclusiva para cada chave de acesso ou identificação de usuários individuais;

b) **chaves de acesso ou identificações:** são códigos de acesso atribuídos a usuários, cada um recebe uma chave de acesso única que pode ser de conhecimento geral. A cada chave de acesso é associada uma senha destinada a autenticar a identidade do usuário que possui essa chave. O mecanismo de chave de acesso permite que ela seja associada a cada recurso que o seu possuidor tenha o direito de acessar, possibilitando a responsabilização individual de cada usuário;

c) **lista de acesso**: mecanismo usado para controlar o acesso de usuários a recursos. Constitui uma espécie de tabela onde constam o tipo e o nome do recurso, ao qual são associadas identificações de usuários com os tipos de operações permitidas aos mesmos;

d) **operações:** determinam o que cada usuário pode fazer em relação a determinado recurso. São normalmente as seguintes: leitura, gravação, alteração, exclusão, eliminação (do meio físico), execução (de algum *software*);

e) **privilégios:** dentro do controle de acesso, determinados usuários têm privilégios de acesso relacionados com as funções exercidas, isto é, quanto maiores os privilégios de acesso, maior o grau hierárquico do seu detentor;

f) **ferramentas de segurança**: ferramental usado para controlar o acesso de usuários aos acervos de informações. Constituem um sistema de programas que executa o controle de acesso dentro de determinado ambiente de informações. Porém existem também os mecanismos não relacionados diretamente à

informática, mas que podem ser utilizados em conjunto, tais como aparelhos de biometria;

g) **categoria**: é o mecanismo que permite classificar usuários, propiciando a segregação dos mesmos à parte do ambiente, normalmente com estruturas de nível hierárquico;

h) **nível hierárquico:** é o mecanismo que permite classificar usuários com categorias similares, propiciando a segregação dos mesmos a partes do ambiente, a exemplo das forças armadas.

Apesar dos esforços que se possa ter despendido em segurança lógica, limitando acessos e protegendo dados, um plano de segurança jamais seria completo se não fossem observados aspectos de segurança física. A segurança física relaciona-se diretamente com os aspectos associados ao acesso físico a recursos de informações, tais como disponibilidade física ou o próprio acesso físico, sejam esses recursos as próprias informações, seus meios de suporte e armazenamento ou os mecanismos de controle de acesso às informações.

Acesso ou posse de um ativo, do ponto de vista físico, é o uso que se faz de determinado recurso. Esse acesso físico está representado, no caso de informações, pelo acesso ao meio de registro ou suporte que abriga as informações. Ainda que mais perceptível e aparentemente sujeito a mais riscos que o acesso lógico, na realidade o acesso físico é muito menos sujeito a riscos; entretanto, o controle pode ser mais difícil, já que depende muito mais de intervenção humana. Normalmente, os riscos relacionados com o acesso físico afetam os meios de registros e suporte das informações, ao passo que os riscos relacionados com o acesso lógico afetam o conteúdo.

Um outro aspecto importante a ser considerado é um programa global destinado a manter o ambiente de informações da organização totalmente seguro contra quaisquer ameaças à sua integridade e sobrevivência, o qual é chamado de plano de contingência. Esse consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre, que os procedimentos de segurança não conseguiram evitar.

Ainda associadas à segurança física e aos planos de contingência, existem os conceitos de preservação e recuperação de informações e seus ativos e meios de suporte. O

conceito de preservação está ligado à necessidade de sobrevivência dos acervos de informações, evitando eventos que causem sua destruição. O conceito de recuperação, entretanto, aplica-se a recursos que tenham sido destruídos ou danificados, permitindo que os mesmos sejam novamente disponibilizados para uso.

3.2 GERENCIAMENTO DE SEGURANÇA DE INFORMAÇÕES – BS 7799

O início da década de 90 marca o começo da terceira etapa do mundo organizacional. É a era da informação, que surge com tremendo impacto provocado pelo desenvolvimento tecnológico e com a chamada tecnologia da informação. A nova riqueza passa a ser o conhecimento, o recurso mais importante substituindo o capital financeiro e, em seu lugar, surge o capital intelectual.

A informação torna-se a principal fonte de energia dentro das organizações e a mais cobiçada também. Na era da informação, as coisas mudam rápida e incessantemente, e quem tem informação passa a ter o poder. Poder de conhecer o concorrente, poder de resolver mais rápido um problema e poder de aprender com os seus erros mais facilmente. E esse bem tão valioso não deixa de ser perseguido de forma correta ou de forma ilícita, e precisa ser protegido. Sua proteção não fica só na condição de evitar que a informação seja roubada, mas também que ela esteja sempre disponível quando necessária, para quem tem autorização para utilizá-la e recuperada com agilidade e com confiabilidade.

A norma *British Standard* (BS) 7799, criada na Inglaterra em 1995, define diretrizes para a implantação de um Sistema de Gerenciamento de Segurança de Informações, cujo objetivo principal é garantir a integridade, confiabilidade e disponibilidade da informação. Para isso é necessário que a organização identifique e defina os seguintes dispositivos para gestão da segurança da informação em conformidade com a Norma BS 7799, que orientam a implementação de um sistema de gestão de segurança da informação: análise de vulnerabilidades, política de segurança, classificação da informação, plano de continuidade de negócios e auditorias do sistema. Tais dispositivos serão detalhados a seguir.

A **Análise de Vulnerabilidades** tem o propósito de mapear as vulnerabilidades da organização, definindo e priorizando ações preventivas e corretivas. Leva-se em conta as características físicas, tecnológicas e humanas do negócio, considerando os processos de

negócio relevantes. Identificam-se ameaças, vulnerabilidades e riscos associados à segurança da informação.

A **Elaboração da Política de Segurança** tem o propósito de desenvolver diretrizes, normas, procedimentos e instruções de segurança para o manuseio, armazenamento, transporte e descarte de informações. Cumpre o papel de formalizar parâmetros e oficializar um código de conduta no trato da informação. A política de segurança tem alto grau de importância no modelo de gestão como um todo.

A **Classificação da Informação** define o melhor tratamento considerando a sensibilidade de cada tipo de informação em todo seu ciclo de vida: manuseio, armazenamento, transporte e descarte. A partir dessa classificação, estabelecem-se normas e procedimentos para classificação da informação, os quais se tornam partes integrantes da política de segurança.

O **Plano de Continuidade de Negócios** tem o propósito de desenvolver estratégias e alternativas de contingência para minimizar os impactos de um incidente de segurança que interfira na continuidade dos negócios. Contempla o levantamento e a análise de processos, visando à criação de um *Business Impact Analisys* (BIA) e a criação, conforme as estratégias escolhidas, de planos de continuidade operacional, planos de recuperação de desastres e programas de administração de crises, assim como testes e simulações.

As **Auditorias no Sistema de Segurança da Informação** podem ser feitas utilizando-se teste de invasão ou processos formais de auditoria em conformidade com os procedimentos da própria BS 7799. O Teste de Invasão tem o propósito de comprovar a existência de vulnerabilidades graves em um ambiente previamente definido como alvo, a fim de validar a solução de segurança implementada ou para chamar a atenção a situações de alto risco.

O desenvolvimento e a implantação de um Sistema de Gerenciamento de Segurança de Informações (SGSI), além da organização da documentação, exige a implementação de controles para atender aos objetivos de segurança da organização. Para isso devem ser executados os seguintes passos segundo a norma BS 7799:

a) **definição da política de segurança da informação**: documento que contém de forma clara e resumida as premissas e diretrizes do Sistema de Gestão de Segurança da Informação;

b) **definição do escopo do sistema de gestão de segurança da informação**: é o perímetro de abrangência que define os ativos que serão contemplados no SGSI, sejam eles sistemas, dispositivos físicos, processos ou ações do pessoal envolvido;

c) **análise do risco**: abrange a identificação das ameaças e vulnerabilidades para os ativos cobertos pelo escopo definido, seus possíveis impactos no negócio. A metodologia utilizada para elaboração dessa análise deve ser documentada, os critérios para identificação dos riscos precisam ser registrados e inseridos no sistema de documentação;

d) **gestão do risco:** definição do processo de gestão dos riscos identificados e critérios para atribuição das prioridades e relação custo benefício de cada ação recomendada;

e) seleção dos controles a serem implementados e seus respectivos objetivos;

f) **preparação da declaração de aplicabilidade**: é a justificativa clara de quais itens da Norma BS 7799 são aplicáveis e serão desdobrados dentro do Sistema de Gestão de Segurança de Informações da organização. Esse passo resume os passos anteriores e complementa o escopo para certificação. É também um norte para evitar que se definam controles em excesso ou que se deixe desprotegido algum ativo importante para a organização.

Estando esses passos bem definidos, a organização pode então iniciar seu processo de implantação dos requisitos contidos na BS 7799, os quais serão descritos de forma objetiva neste capítulo. Os requisitos são:

a) **política de segurança da informação**: prover à direção uma orientação e apoio para a 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;

b) **infra-estrutura da segurança da informação**: gerenciar a segurança dentro da organização. Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização;

c) **segurança no acesso de prestadores de serviço**: manter a segurança dos recursos de processamento de informação e ativos de informação organizacionais acessados por prestadores de serviço. Convém que seja controlado o acesso de prestadores de serviços aos recursos de processamento da informação da organização;

d) **terceirização:** manter a segurança da informação quando a responsabilidade pelo processamento da informação é terceirizada para uma outra organização. Convém que o acordo de terceirização considere riscos, controles de segurança e procedimentos para os sistemas de informação, rede de computadores e/ou estações de trabalho no contrato entre as partes;

e) **contabilização dos ativos**: manter a proteção adequada dos ativos da organização. Convém que todos os principais ativos de informação sejam inventariados e tenham um proprietário responsável;

f) **classificação da informação**: assegurar que os ativos de informação recebam um nível adequado de proteção. Convém que a informação seja classificada para indicar a importância, a propriedade e o nível de proteção;

g) **segurança na definição e nos recursos de trabalho:** reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações. Convém que responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de cada contrato de trabalho;

h) **treinamento dos usuários:** assegurar que os usuários estejam cientes das ameaças e das preocupações de segurança da informação e estejam equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho. Convém que usuários sejam treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança;

i) **respondendo aos incidentes de segurança e ao mau funcionamento:** minimizar danos originados pelos incidentes de segurança, e mau funcionamento, e monitorar e aprender com tais incidentes. Convém que os incidentes que afetam a segurança sejam reportados através dos canais apropriados o mais rapidamente possível;

j) **áreas de segurança:** prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização. Convém que os recursos e as instalações de processamento de informações, críticas ou sensíveis do negócio, sejam mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Convém que estas sejam fisicamente protegidas de acesso não autorizado, dano ou interferência;

k) **segurança dos equipamentos:** prevenir perda, dano ou comprometimento dos ativos, e a interrupção das atividades do negócio. Convém que os equipamentos sejam fisicamente protegidos contra ameaças à sua segurança e perigos ambientais. A proteção dos equipamentos é necessária para reduzir o risco de acessos não autorizados a dados e para proteção contra perda ou dano;

l) **controles gerais**: evitar exposição ou roubo de informação e de recursos de processamento da informação. Convém que informações e recursos de processamento da informação sejam protegidos de divulgação, modificação ou roubo por pessoas não autorizadas, e que sejam adotados controles de forma a minimizar sua perda ou dano;

m) **procedimentos e responsabilidades operacionais:** garantir a operação segura e correta dos recursos de processamento da informação. Convém que os procedimentos e as responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos;

n) **planejamento e aceitação dos sistemas:** minimizar o risco de falhas nos sistemas. Convém que projeções de demanda de recursos e de carga de máquina futura sejam feitas para reduzir o risco de sobrecarga dos sistemas;

o) **proteção contra software malicioso:** proteger a integridade do software e da informação. É necessário que se adotem precauções para prevenir e detectar a introdução de *softwares* maliciosos;

p) ***housekeeping***: manter a integral disponibilidade dos serviços de comunicação e processamento da informação. Convém que sejam estabelecidos procedimentos de rotina para a execução das cópias de segurança e para a disponibilização dos recursos de reserva, conforme definido na estratégia de contingência, de forma a viabilizar a restauração em tempo hábil, controlando e registrando eventos e falhas e, quando necessário, monitorando o ambiente operacional.

q) **gerenciamento de rede**: garantir a salvaguarda das informações na rede e a proteção da infra-estrutura de suporte. O gerenciamento de segurança de rede que se estendam além dos limites físicos da organização requer particular atenção;

r) **segurança e tratamento de mídias:** prevenir danos aos ativos e interrupções das atividades do negócio. Convém que as mídias sejam controladas e fisicamente protegidas;

s) **troca de informação e *software***: prevenir a perda, modificação ou mau uso de informações trocadas entre organizações. Convém que as trocas de informações e *software* entre organizações sejam controladas e estejam em conformidade com toda a legislação pertinente;

t) **requisitos do negócio para o controle de acesso:** controlar o acesso à informação. Convém que o acesso à informação e processos do negócio sejam controlados na base dos requisitos de segurança e do negócio;

u) **gerenciamento de acessos do usuário:** prevenir acessos não autorizados aos sistemas de informação. Convém que procedimentos formais sejam estabelecidos para controlar a concessão de direitos de acesso aos sistemas de informação e serviços;

v) **responsabilidade dos usuários:** prevenir acesso não autorizado dos usuários. Convém que os usuários estejam cientes de suas responsabilidades para a manutenção efetiva do controle de acesso, considerando particularmente o uso de senhas e a segurança de seus equipamentos;

w) **controle de acesso à rede:** proteção dos serviços de rede. Convém que o acesso aos serviços de rede internos e externos seja controlados;

x) **controle de acesso ao sistema operacional:** prevenir acesso não autorizado ao computador. Convém que as funcionalidades de segurança do sistema operacional sejam usadas para restringir o acesso aos recursos computacionais;

y) **controle de acesso às aplicações:** prevenir acesso não autorizado à informação contida nos sistemas de informação. Convém que os recursos de segurança sejam utilizados para restringir o acesso aos sistemas de aplicação;

z) **monitoração do uso e acesso ao sistema**: descobrir atividades não autorizadas. Convém que os sistemas sejam monitorados para detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança;

aa) **computação móvel:** garantir a segurança da informação quando se utilizam a computação móvel e os recursos de trabalho remoto. Convém que a proteção requerida seja proporcional ao risco dessa forma específica de trabalho;

bb) **requisitos de segurança de sistemas**: garantir que a segurança seja parte integrante dos sistemas de informação. Convém que todos os requisitos de segurança, incluindo a necessidade de acordos de contingência, sejam identificados na fase de levantamento de requisitos de um projeto e justificados, acordados e documentados como parte do estudo de caso de um negócio para um sistema de informação;

cc) **segurança nos sistemas de aplicação:** prevenir perda, modificação ou uso impróprio de dados do usuário nos sistemas de aplicações. Convém que os controles apropriados e as trilhas de auditoria ou o registro de atividades sejam previstos para os sistemas de aplicação, incluindo as escritas pelos usuários. Convém que estes incluam a validação dos dados de entrada, processamento interno e dados de saída;

dd) **controles de criptografia**: proteger a confidencialidade, autenticidade ou integridade das informações;

ee) **segurança de arquivos do sistema**: garantir que projetos de tecnologia de informação e as atividades de suporte sejam conduzidos de modo seguro. Convém que o acesso aos arquivos do sistema seja controlado;

ff) **segurança nos processos de desenvolvimento e suporte**: manter a segurança do software e da informação do sistema de aplicação. Convém que os ambientes de desenvolvimento e suporte sejam rigidamente controlados;

gg) **aspectos da 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. Convém que o processo de gestão da continuidade seja implementado para reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas de segurança através da combinação de ações de prevenção e recuperação;

hh) **conformidade com requisitos legais**: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança. Convém que consultoria em requisitos legais específicos seja procurada em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais;

ii) **análise crítica da política de segurança e da conformidade técnica**: garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança. Convém que a segurança dos sistemas de informação seja analisada criticamente em intervalos regulares;

jj) **considerações quanto à auditoria de sistemas**: maximizar a eficácia e minimizar a interferência no processo de auditoria de sistema. Convém que existam controles para a salvaguarda dos sistemas operacionais e ferramentas de auditoria durante as auditorias de sistema.

Com os requisitos acima apresentados, uma organização pode trabalhar na redução dos incidentes relacionados à segurança de informações, procurando resguardar os seus ativos mais importantes. Consta também na própria BS 7799 que a aplicação desses controles não deve ser considerada como o passo definitivo no que tange à segurança de informações, podendo a própria empresa definir e implementar algum outro controle não citado acima.

3.3 ATUALIDADE EM SEGURANÇA DE INFORMAÇÕES

A velocidade das mudanças da economia digital tem gerado uma demanda crescente por soluções de segurança mais complexas, que garantam um nível mínimo de proteção para toda a estrutura tecnológica e organizacional, com custo reduzido e no menor tempo possível.

Uma vez conectada à Internet, a rede de computadores de qualquer organização fica potencialmente acessível a usuários externos, incluindo *hackers* com intenção maliciosa. Aliado a isso, o ambiente de rede das grandes empresas envolve hardware, sistemas operacionais, protocolos e aplicações de diversos fornecedores, fazendo com que a rede passe a ter vulnerabilidades adicionais, que podem ser exploradas por um usuário não-autorizado, seja ele interno ou externo.

Um fracasso na proteção das informações pode resultar em prejuízo financeiro significativo, na perda de segmentos de mercado e em danos irreparáveis à imagem da empresa. Os riscos dessa insegurança são reais, e as empresas de tecnologia e as indústrias são as mais atingidas.

Em recente relatório da *Bear Stearns* (MÓDULO, 2002), as previsões para o comércio eletrônico *business-to-business* (B2B) apontam para um mercado de US$ 1,1 trilhão em 2003, destacando que a maioria dos *players* do mercado não possui estrutura de segurança para seus negócios. Nos próximos anos essas companhias deverão construir infra-estruturas completas de segurança para suas operações.

As projeções da *Forrester Research* (MÓDULO, 2002) para o mercado mundial business-to-business (B2B) em 2003, estimam que 90% das vendas totais de comércio eletrônico (US$ 1,4 trilhão) sejam de transações B2B (US$ 1,3 trilhão) e cerca de 10% (US$ 108 bilhões) para *business-to-client* (B2C). Pesquisa realizada pelo IDC mostra que os gastos via Internet na América Latina deverão atingir US$ 8 bilhões em 2003.

O mercado *business-to-business* brasileiro deverá movimentar, ainda de acordo com pesquisa do IDC, US$ 1,9 bilhão em 2003 (MÓDULO, 2002). O mercado de *e-commerce* no Brasil deverá sofrer crescimento exponencial, com destaque para as negociações entre empresas. O Brasil atualmente tem uma participação substancial com 88% desse mercado seguido pelo México com 6% e pela Argentina com 2% das vendas. Um dos principais fatores

do atual estágio de desenvolvimento do comércio eletrônico, no Brasil, é a sofisticação dos sistemas bancários, com mais de 1,5 milhão de correntistas que acessam suas contas através de PCs conectados via linha direta ou por Internet.

A Sétima Pesquisa Nacional sobre Segurança da Informação (MÓDULO, 2001), realizada com 165 executivos de grandes empresas públicas e privadas, distribuídas entre os segmentos financeiro, serviços, informática, indústria, telecomunicações, governo, *e-commerce* e varejo, indicou que 40% das grandes empresas brasileiras já sofreram ataques eletrônicos (número bem maior que o ano anterior que foi de 32%), sendo que 43% dessas empresas sofreram os ataques no segundo semestre de 2001. Entretanto, 31% delas não sabem precisar se suas redes já foram ou não invadidas. Ainda assim, 46% das empresas não têm um plano de ação contra ataques, evidenciando o potencial de crescimento desse mercado. Em relação ao orçamento total para informática para o ano de 2000, 80% das empresas afirmaram que seu orçamento de segurança aumentaria para no ano de 2001. Dentre as empresas que declararam os investimentos planejados para 2001, 14% reservam mais de um quinto do orçamento de TI para segurança de informações.

Na oitava edição (MÓDULO, 2002), a pesquisa apresenta um panorama do segmento de segurança da informação no país, com dados estatísticos sobre o mercado, indicadores, melhores práticas e uma análise das informações através de gráficos dos resultados das diversas questões levantadas.

Observa-se neste trabalho que, ano após ano, cresce a preocupação das empresas com a proteção de suas informações, aumentando também a adoção de controles para minimizar os riscos resultantes de ameaças e vulnerabilidades. A amostra desse ano dobrou em relação à de 2001, o que revela a importância e a credibilidade que este trabalho vem conquistando junto ao mercado nacional.

A pesquisa quantitativa foi desenvolvida a partir de uma amostra de 547 questionários presenciais coletados entre março e agosto de 2002, junto a profissionais ligados à área de tecnologia e segurança da informação de diversos segmentos de negócios – Bancos (21%), Governo (19%), Informática (15%), Indústria e Comércio (15%), Serviços (10%), Energia (10%), Telecomunicações (9%) e Saúde (1%), correspondendo a mais de 30% das mil maiores empresas brasileiras. O questionário foi composto por 40 questões objetivas, sendo algumas de respostas múltiplas. Foram computadas somente as perguntas efetivamente

respondidas. Essa pesquisa nacional de segurança da informação, mostra que, embora as organizações reconheçam a importância da segurança da informação como a melhor forma de garantir a manutenção dos negócios, as principais soluções implementadas ainda têm características técnicas e pontuais, como a utilização de antivírus e *firewall*.

Outro fato relevante é que mais da metade das empresas brasileiras não têm planos de ação formalizados em caso de ataques, apesar da expectativa de aumento nos problemas com a segurança e o crescimento no índice de registros de ataques e invasões. A ausência de procedimentos emergenciais amplia a extensão do problema, deixando as empresas mais vulneráveis e aumentando o impacto sobre os negócios. A pesquisa revela que a falta de conscientização é ainda a grande barreira para a implementação da segurança da informação, embora tenha ficado claro que o investimento em capacitação para a formação de profissionais será um dos principais investimentos para 2002 e 2003.

A figura do *Security Officer* vem se consolidando como o principal gestor da segurança nas empresas. Outro aspecto importante apresentado é a falta de procedimentos internos de análise e investigação que facilitem a identificação da causa dos problemas, bem como uma quantificação mais precisa dos prejuízos. Cerca de 56% das empresas no Brasil não conseguem quantificar suas perdas financeiras com problemas de segurança da informação.

No que se refere à oferta de produtos e serviços voltados para a segurança da informação, o mercado encontra-se satisfatoriamente abastecido para as demandas identificadas até o presente momento, principalmente no que se refere às ferramentas e soluções tecnológicas.

Para desenvolver a segurança da informação no Brasil, sensibilizando as organizações para a implementação de medidas preventivas, que reduzam os riscos, é preciso haver uma conjunção entre Tecnologia (recursos físicos e lógicos), Pessoas (cultura, capacitação e conscientização) e Processos (metodologia, normas e procedimentos). Estabelecer recomendações sobre controles e práticas envolvendo esses três elementos é o principal objetivo da ISO17799 e da BS 7799, conjunto de normas e padrões de gerenciamento para implementação de práticas de segurança da informação. Essa é uma prática que se encontra em processo de adoção em mais de 20 países, devendo se tornar um padrão adotado mundialmente nos próximos anos. De acordo com o *Yankee Group*

(MÓDULO, 2001), invasões, como as ocorridas nas gigantes *Yahoo*, *eBay*, *Etrade*, *Buy.com* e *Amazon.com*, vão gerar perdas de aproximadamente US$ 1 bilhão. Estima-se que apenas essas empresas atacadas gastaram entre US$ 100 milhões e US$ 200 milhões para atualizar seus sistemas de segurança durante o ano de 2000.

Pesquisa do Gartner (MÓDULO, 2001), realizada com 589 empresas do mundo todo entre março e junho de 2001, mostra que 56% dos entrevistados pretendiam gastar mais com tecnologia da informação em 2001 do que gastaram em 2000. A mesma pesquisa descobriu que a situação econômica não impediu que empresas do "Tipo A", ou que adotam tecnologia de ponta, aumentassem seus orçamentos, baseando-se em uma porcentagem de suas vendas. O governo, que é considerado do "Tipo A", em função dos projetos de e-governo apresenta um aumento de 18% entre 2000 e 2002, seguido pelos serviços de telecomunicações onde esperava-se um aumento de 13.9% em gastos com sistemas de informação e do setor bancário que estava planejando um crescimento de orçamento de ativos na ordem de 10,8%.

As estimativas de mercado divulgadas por vários órgãos, mesmo que apresentem diferenças numéricas evidentes, apontam para a mesma direção: crescimento do setor no mundo. Para o *Yankee Group* (MÓDULO, 2001), o mercado de segurança mundial saltaria de US$ 3,6 bilhões em 1999 para US$ 10,8 bilhões em 2003. Segundo o *Datamonitor* (MÓDULO, 2002), os investimentos em segurança eletrônica deverão ser de US$ 15,44 bilhões no ano 2003. Já o *Bear Stearns* (MÓDULO, 2002) estima um mercado de US$ 20,9 bilhões em 2005 e acredita que o setor de segurança da Internet deva entrar em um forte ciclo de crescimento na próxima década.

O *International Data Corporation* – IDC – divulgou previsão de crescimento de 25% ao ano para o mercado de serviços relacionados à segurança de redes nos próximos cinco anos. O crescimento do comércio eletrônico também se configura como um grande gerador de demanda para serviços de segurança.

Define-se como *Application Service Providers* (ASPs) as empresas que disponibilizam, hospedam, gerenciam e alugam software a partir de uma localização centralizada. Utilizam o modelo de negócios *one-to-many* e tipicamente são acessadas pela Internet ou por um acesso dedicado. Segundo relatório do IDC, o mercado geral de ASPs chegará a US$ 23 bilhões em 2003. É importante mencionar, no entanto, que, por se tratar de um ramo ainda não explorado, mesmo em nível mundial, o segmento de ASP voltado para a

segurança não dispõe de estatísticas que possibilitem a determinação de seu potencial de crescimento.

Segundo o IDC, apoiado no crescimento do comércio eletrônico e no aumento das ameaças internas, o mercado mundial de software de segurança para a Internet alcançará US$ 11,3 bilhões em 2004. Esse mercado evoluiu historicamente de US$ 1,2 bilhões em 1996, para 2 bilhões em 1997, 3,1 bilhões em 1998, atingindo 4,0 bilhões em 1999.

3.4 APLICAÇÃO DA BS 7799 NAS EMPRESAS

Existem atualmente em torno de quinhentas empresas certificadas em BS 7799 no mundo (http://www.xisec.com), e por se tratar de um assunto sensível no mercado, a maioria destas empresas evita a divulgação e o acesso as informações de implementação dos seus Sistemas de Gerenciamento de Segurança de Informações, assim como o resultado desta implementação. Por estas razões é limitado o número de exemplos de aplicações que se pode obter na literatura, um caso é apresentado abaixo.

3.4.1 *Aplicação na T-Systems CSM*

Um dos exemplos da aplicação da Norma BS 7799 é a empresa de telecomunicações alemã T-Systems CSM, uma das quatro divisões da *Deutsche Telekom*, que tem como atividades principais o comércio eletrônico, redes corporativas, aplicações de acesso e segurança, soluções individuais de TI e de telecomunicações, além de consultoria gerencial, cuja certificação foi realizada no ano de 2000. Essa organização foi assessorada pela empresa de consultoria em segurança de informações *Aexis* (http://www.aexis.de), segundo a direção da empresa, a preparação, implementação e certificação da empresa passaram pelas seguintes etapas:

a) **escopo da certificação:** todas as atividades da T-Systems CSM foram cobertas pelo Sistema de Gerenciamento de Segurança de Informações, considerando dezessete unidades localizadas por toda a Alemanha, totalizando 6.500 funcionários. Dessa forma, a T-Systems CSM era a única companhia na Alemanha com a certificação em todas as suas atividades;

b) **motivação:** garantir a existência de planos de segurança dentro da T-Systems CSM; medir a efetividade do uso das instalações de processamento da informação; manter a boa imagem da corporação; satisfazer os requisitos dos clientes; atrair novos clientes e manter o diferencial competitivo;

c) **preparação para certificação:** definição do processo de segurança baseado em requisitos e procedimentos; análise de risco de todos os processos internos; seleção dos controles; implementação dos controles e estabelecimento do gerenciamento da segurança; planejamento do processo de auditoria; criação de uma equipe eficiente de projeto com competências pessoais; documentação completa do processo de segurança, levando em conta as modificações em outros processos; obtenção da aprovação e recursos necessários por parte da direção; realização de acordos com outros comitês;

d) **análise de risco**: usado plano de segurança existente; estimativa dos riscos remanescentes; cada objeto (técnico ou *software*) dentro da T-Systems CSM teve um plano de segurança; esses planos estimavam os riscos remanescentes após os controles de segurança implementados; responsáveis são os donos do objeto;

e) **plano de continuidade do negócio:** recuperação de dados e disponibilidade de serviços; sistemas espelhados e planos de recuperação de desastres;

f) **acordos contratuais:** acordos dos níveis de serviço; identificação das necessidades para manter os acordos contratuais;

g) **conscientização:** a conscientização do pessoal é a chave para o sucesso; toda a organização foi treinada; *slogans*; *posters*; artigos em revistas internas; publicações na Intranet; todos conheciam a BS 7799 e a importância da segurança de informações;

h) **certificação:** realização de duas pré-auditorias em unidades diferentes; quatro e dois meses antes da certificação; certificação emitida em novembro/2000; realizadas mais de 350 entrevistas em muitas unidades que foram visitadas; processo de certificação levou 10 meses;

i) **recursos utilizados:** equipe de projeto e trabalho; treinamentos (3 horas para cada funcionário); recursos para implementação dos controles; publicidade; certificadora; atualização permanente dos custos;

j) **os benefícios com a certificação**: atender aos requisitos dos clientes; reforçar a imagem da companhia; demonstrar segurança e conquistar novos clientes; melhor conhecimento para a segurança; aumento da qualificação dos colaboradores; reconhecimento internacional.

No Brasil, a primeira organização certificada foi uma empresa de consultoria de segurança de informações. A empresa foi certificada pela *Det Norske Veritas* (DNV) – organismo certificador. O processo de auditoria executado na referida empresa é objeto de estudo deste trabalho.

Os conceitos gerais sobre segurança, as bases que levaram ao surgimento da Norma BS 7799, os requisitos necessários para tal implantação e o caso de sucesso, apresentados neste capítulo, reportam ao objetivo geral deste estudo, que pretende determinar a dimensão do cenário que um processo de auditoria deve avaliar e considerar no âmbito de cada organização. O método de pesquisa, seus detalhes, as etapas, os instrumentos e ajustes são detalhados no capítulo 4.

CAPÍTULO 4

4 METODOLOGIA DE PESQUISA

O objetivo deste capítulo é definir o método utilizado para a realização da pesquisa, seus detalhes, instrumentos e ajustes, o cenário de realização do estudo e a relevância para essa empresa da BS 7799 e para os seus profissionais.

4.1 MÉTODO DE PESQUISA

Conforme Yin (2001), a escolha da estratégia adequada de pesquisa está relacionada a três condições: o tipo de questão de pesquisa proposto; a extensão de controle que o pesquisador tem sobre eventos comportamentais efetivos e o grau de enfoque em acontecimentos históricos em oposição a acontecimentos contemporâneos (ver Figura 4).

Estratégia	Forma da questão de pesquisa	Exige controle sobre eventos comportamentais?	Focaliza acontecimentos contemporâneos?
Experimento	como, por que	sim	sim
Levantamento	quem, o que, onde, quantos, quanto	não	sim
Análise de arquivos	quem, o que, onde, quantos, quanto	não	sim/não
Pesquisa histórica	como, por que	não	não
Estudo de caso	como, por que	não	sim

Fonte: Yin (2004)

Figura 4 Situações relevantes para diferentes estratégias de pesquisa

Considerando a forma da questão de pesquisa do presente estudo (como); a não exigência de controle sobre eventos comportamentais e o enfoque em acontecimentos contemporâneos, optou-se pelo método de estudo de caso para a realização da presente pesquisa.

Considerando ainda que, no Brasil, a primeira empresa que auditou um Sistema de Gerenciamento de Segurança de Informações com base na Norma BS 7799 foi a *Det Norske Veritas* (DNV), esta foi escolhida como objeto do estudo de caso da presente pesquisa.

Dentro desse contexto, além da revisão da literatura, as etapas planejadas para este estudo de caso foram:

a) coleta de dados;

b) coleta de evidências;

c) análise das evidências;

d) geração do relatório.

A Figura 5 apresenta o desenho da pesquisa.

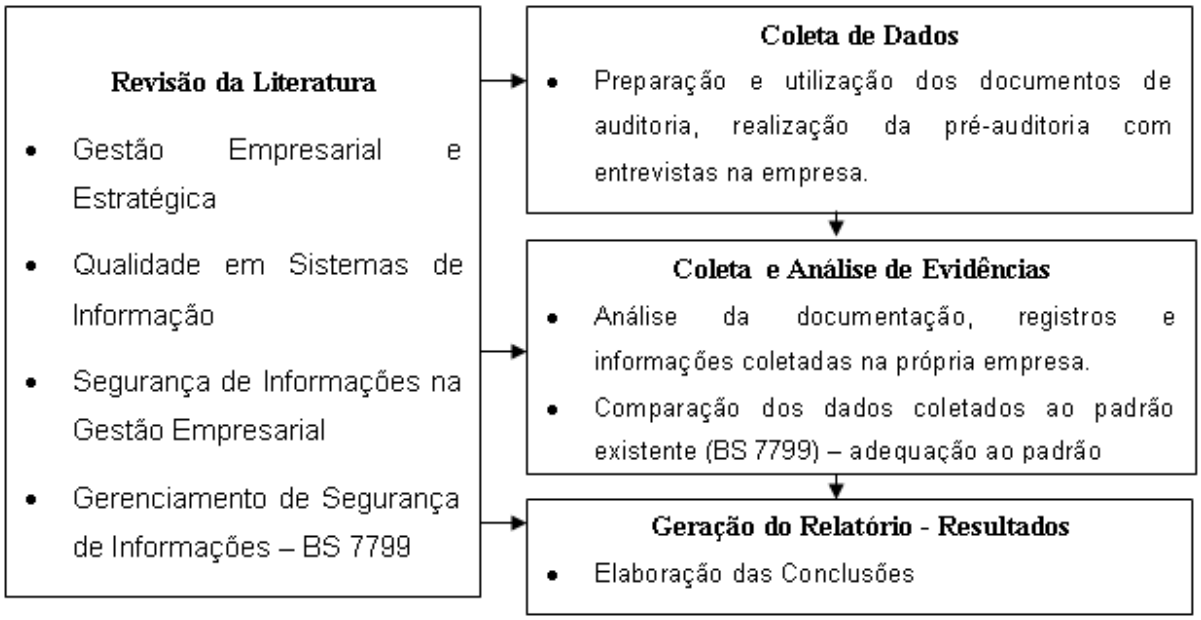


Figura 5 Desenho da pesquisa

4.1.1 *Coleta de Dados*

A preparação para a coleta de dados pode ser uma atividade complexa e difícil, se não for realizada corretamente. Todo o trabalho de investigação do estudo de caso poderá ser posto em risco (YIN, 2001). Uma boa preparação começa com as habilidades desejadas por parte do pesquisador; entretanto, não existem mecanismos do tipo testes, exame da ordem ou vestibular para avaliar as habilidades necessárias a um estudo de caso. Entretanto, uma lista básica de habilidades comumente exigidas incluiria:

a) uma pessoa capaz de fazer boas perguntas e interpretar respostas;

b) uma pessoa que seja boa ouvinte e não seja enganada por suas próprias ideologias e por preconceitos;

c) uma pessoa capaz de ser adaptável e flexível, que vislumbre oportunidades e não ameaças;

d) uma pessoa que seja capaz de manter o foco na questão relevante do assunto;

e) uma pessoa imparcial em relação a noções preconcebidas e provas contraditórias.

Um segundo tópico importante é o treinamento e preparação para um estudo em específico, o objetivo desse treinamento é que o pesquisador saiba:

a) por que o estudo está sendo realizado;

b) quais provas estão sendo procuradas;

c) quais variações podem ser antecipadas (e o que deve ser feito se essas variações ocorrerem);

d) o que constituiria uma prova contrária ou corroborativa para qualquer proposição dada.

Uma das funções do treinamento, segundo o autor, é a de estabelecer um protocolo a respeito do estudo proposto, ou seja, estabelecer uma minuta dos assuntos que devem ser tratados no estudo de caso. Tal protocolo deve apresentar as seguintes seções:

a) visão geral do projeto do estudo de caso;

b) procedimento de campo;

c) questões específicas do estudo de caso;

d) guia para o relatório do estudo de caso.

A preparação final para a realização da coleta de dados, segundo Yin (2001), é a realização de estudo de caso-piloto para auxiliar o pesquisador a aprimorar os planos para a coleta de dados tanto em relação ao conteúdo dos dados quanto aos procedimentos que devem ser seguidos.

Neste estudo de caso, a fase de coleta de dados foi realizada pela função do auditor/coordenador da norma em questão, o qual possui as habilidades e o treinamento necessários para avaliar o foco da questão do estudo. Sobre a etapa do protocolo proposto por Yin (2001), em certas etapas foram utilizados os formulários do modelo internacional da DNV para a coleta das informações do cliente, e em outras, apenas uma lista de verificação de assuntos, a fim de comprovar se a etapa havia sido completada de forma satisfatória.

O estudo de caso-piloto, não foi aplicado neste trabalho, em virtude da própria documentação utilizada e definida pelos procedimentos padrões ter suprido a necessidade de validar a coleta de dados.

4.1.2 *Coleta de Evidências*

As evidências para um estudo de caso podem surgir de seis fontes distintas: documentos, registros em arquivo, entrevistas, observação direta, observação participante e artefatos físicos (YIN, 2001).

Documento – exceto para os estudos que investigam sociedades que não dominavam a arte da escrita, é provável que as informações documentais sejam relevantes a todos os tópicos do estudo de caso. Para os estudos de caso, o uso mais importante de documentos é corroborar e valorizar as evidências oriundas de outras fontes;

Registros em arquivo – para muitos estudos de caso, os registros em arquivo geralmente em sua forma computadorizada também podem ser muito importantes. Quando se julga que as provas de arquivos sejam importantes, o pesquisador deve tomar cuidado ao averiguar sob quais condições elas foram produzidas e qual seu grau de precisão;

Entrevistas – uma das mais importantes fontes de informações para um estudo de caso são as entrevistas. No geral, as entrevistas constituem uma fonte essencial de evidências para estudos de caso, já que a maioria delas trata de questões humanas. Essas questões deveriam ser registradas e interpretadas por meio dos olhos de entrevistadores específicos, e respondentes bem-informados podem dar interpretações importantes para uma determinada situação. As entrevistas, no entanto, devem sempre ser consideradas apenas como relatórios verbais e, como tal, uma abordagem razoável é a de corroborar os dados obtidos em entrevistas com informações obtidas de outras fontes;

Observação direta – ao realizar uma visita de campo ao local escolhido para o estudo de caso, cria-se a oportunidade de realizarem-se observações diretas. Assumindo-se que os fenômenos de interesse não sejam puramente de caráter histórico, encontrar-se-ão disponíveis para observação alguns comportamentos ou condições ambientais relevantes. Essas observações servem como outra fonte de evidências em um estudo de caso;

Observação participante – é uma modalidade especial de observação na qual o pesquisador não é apenas um observador passivo, em vez disso, assume uma variedade de funções dentro de um estudo de caso e pode, de fato, participar de eventos que estão sendo estudados;

Artefatos físicos – uma última fonte de evidências é um artefato físico ou cultural, um aparelho de alta tecnologia, uma ferramenta ou instrumento, uma obra de arte ou alguma outra evidência física. Pode-se coletar ou observar esses artefatos como parte de uma visita de campo e pode-se utilizá-los extensivamente na pesquisa.

No estudo de caso proposto, as evidências foram coletadas de documentos, registros, entrevistas e observação participante. Devido à finalidade da atividade de auditoria de sistemas, os documentos são base da metodologia de auditoria proposta pela DNV que especifica as etapas a serem conduzidas tanto pela equipe comercial quanto pela equipe auditora que realiza a verificação *in loco*. Os registros são as informações geradas pelo cliente que responde aos formulários utilizados para levantamento de informações, a fim de preparar a proposta comercial e também as informações geradas do Sistema de Gestão de Segurança de Informações (SGSI) e da própria auditoria. As entrevistas servem para corroborar as informações que foram identificadas nos documentos e/ou registros, e por fim, a observação participante devido à execução da auditoria propiciar a observação e interação com evidências

para comprovação das informações relacionadas anteriormente em documentos e registros do SGSI.

4.1.3 *Análise de Evidências*

Segundo Yin (2001), a análise de evidências consiste em examinar, categorizar, classificar em tabelas ou, do contrário, recombinar as evidências considerando as proposições iniciais de um estudo. Quatro técnicas analíticas dominantes devem ser utilizadas: adequação ao padrão, construção da explanação, análise de séries temporais e modelos lógicos de programa. Cada uma delas pode ser aplicável em projetos de estudo de caso único ou de casos múltiplos, e cada estudo deve levar essas técnicas em consideração.

Adequação ao padrão – uma das estratégias mais desejáveis é a utilização da lógica de adequação ao padrão, essa lógica (TROCHIM *apud* YIN, 2001) compara um padrão fundamentalmente empírico com outro de base prognóstica (ou com várias outras previsões alternativas). Se os padrões coincidirem, os resultados podem ajudar o estudo de caso a reforçar sua validade interna;

Construção da explanação – uma segunda estratégia analítica constitui um tipo especial de adequação ao padrão, o procedimento tem como objetivo analisar os dados do estudo construindo uma explanação sobre o caso. A elaboração gradual de uma explanação assemelha-se ao processo de aprimorar um conjunto de idéias, nas quais um aspecto importante é, novamente, levar em consideração outras explanações plausíveis ou concorrentes. Nesse sentido, a explanação final pode não ter sido inteiramente estipulada no começo de um estudo e, por conseguinte, pode diferir, nesse sentido, da abordagem de adequação ao padrão previamente descrita. Em vez disso, as evidências do estudo de caso são examinadas, os posicionamentos teóricos são revisados, e as evidências são examinadas novamente de uma nova perspectiva, nesse modo iterativo;

Análise de séries temporais – outra estratégia analítica é conduzir uma análise de séries temporais, diretamente análoga à análise de séries temporais realizadas em experimentos e em pesquisas quase-experimentais. Uma análise como essa pode seguir muitos padrões. Quanto mais complicado e preciso for o padrão, mais a análise de séries temporais estabelecerá uma base firme para as conclusões do estudo de caso;

Modelos lógicos de programa – esta estratégia na verdade é uma combinação das técnicas de adequação ao padrão e de análise de séries temporais. O padrão que está sendo buscado é o padrão-chave de causa e efeito entre variáveis independentes e dependentes. Contudo, a análise estabelece deliberadamente um encadeamento de eventos (padrão) ao longo do tempo (série temporal), dando conta dessas variáveis independentes e dependentes. A estratégia, segundo o autor, é mais útil para estudos de caso explanatórios e exploratórios do que para estudos descritivos.

No estudo proposto neste trabalho, o modelo utilizado foi o de adequação ao padrão, uma vez que a proposta deste estudo é avaliar a adequação da metodologia de aplicação de procedimentos para definição e execução das etapas de um processo de certificação em um Sistema de Gerenciamento de Segurança de Informações em empresa do mercado nacional, considerando que o padrão citado é utilizado no mercado internacional regularmente e com sucesso.

4.1.4 *Geração do Relatório*

O objetivo deste item é ilustrar alguns tópicos que devem ser considerados na composição e na exposição, os quais estão diretamente relacionados ao trabalho.

O relatório de um estudo de caso não segue qualquer fórmula estereotipada, e também não precisa ser apenas na forma escrita. Os estudos de caso têm uma relação mais diversa de possíveis públicos-alvo (colegas, profissionais em geral, grupos especiais, instituição financiadora) do que a maioria dos outros tipos de pesquisa. Sendo assim, uma tarefa essencial, ao se projetar o relatório global do estudo, é identificar cada um dos públicos específicos para o relatório. Cada um deles possui necessidades diferentes, e nenhum relatório em especial atenderá às demandas de todos os públicos simultaneamente. As supostas preferências de um público em potencial devem impor o modelo de um relatório de estudo de caso, o relatório em si deve refletir as ênfases, os detalhes, o modelo de composição e até mesmo a extensão conveniente às necessidades do suposto público.

Quanto às variedades de composição, um relatório de estudo de caso não precisa ser apenas escrito, as informações e os dados obtidos em um caso podem ser expostos de outras maneiras, como uma exposição oral ou até um conjunto de fotos ou gravações de vídeo. A escolha influenciará reciprocamente a tarefa de identificar o público para o estudo de caso. As

seções, os subtópicos e outras partes integrantes de um relatório devem ser organizados de alguma maneira, e essa organização constitui a estrutura ilustrativa do relatório.

Neste estudo de caso, os públicos-alvo são o acadêmico e os profissionais da área de certificação de sistemas de segurança de informações. Em relação à composição do relatório, foi adotada a prática descritiva, com seqüência de subtópicos, com a existência de um problema, revisão da literatura, método, análise dos dados coletados e conclusões a partir dessas análises.

Respeitando a política de segurança das partes, o nome da empresa que teve o seu Sistema de Gerenciamento de Segurança de Informações auditado e que serviu de análise para validação do modelo proposto não será divulgado.

4.1.5 **Det Norske Veritas*: Dados Gerais.***

A DNV foi criada em Oslo, Noruega, em 1864, com a finalidade de garantir, para grupos seguradores, a qualidade na construção de embarcações. Atualmente com 5.500 funcionários de 74 diferentes nacionalidades e mais de trezentos escritórios em todo o mundo, a DNV ajuda seus clientes a gerenciar riscos prestando os seguintes serviços:

a) classificação de plataformas ;

b) certificação/verificação de estruturas fixas offshore e tubulações;

c) garantia de ciclo de vida;

d) certificação de materiais e componentes para indústria offshore;

e) verificação técnica e de conformidade;

f) análise de risco e confiabilidade;

g) gerenciamento de risco ambiental;

h) inspeção baseada em riscos;

i) avaliação, treinamento e certificação relacionada aos sistemas de gerenciamento de segurança, qualidade, meio ambiente, segurança de informações, marca CE, saúde (ONA) dentre outras.

Sua rede internacional está distribuída em áreas de atuação, divididas em regiões. O Brasil se inclui na área de Indústrias em Geral (*General Industry*), Região Américas, mais especificamente na Região América do Sul. A *Det Norske Veritas* (DNV) começou a funcionar no Brasil em outubro de 1974. Antes disso existia na forma de um agente naval que a representava no Porto do Rio de Janeiro. Dessa data até os dias de hoje, pode-se dizer que a DNV passou por três períodos bem distintos.

O primeiro período foi o começo de suas atividades, marcado pela era *offshore*, que predominou até pouco mais da metade da década de 80. O segundo, logo depois até o início dos anos 90, foi seu período de forte atuação na área naval e, por terceiro, o industrial, que se mantém até hoje em função de sua atuação nas certificações de Sistemas de Gestão ISO.

Apesar da atual abrangência de participação da DNV no mercado, seu início no país foi discreto. Começou funcionando nas instalações da Agência Marítima Grieg. Naquela ocasião, seu quadro técnico era composto apenas por dois vistoriadores navais, um deles era o próprio gerente da região.

As atividades do gerente da região resumiam-se a idas a bordo de navios que aqui aportavam, com o objetivo de efetuar vistorias, possibilitando que as embarcações permanecessem em classe. A descoberta de petróleo na Bacia de Campos levou a Petrobras a pesquisar no mundo empresas envolvidas com prestação de serviços relacionados à atividade *offshore*. A destacada atuação da DNV no Mar do Norte, como certificadora de plataformas, foi fator decisivo para que fosse feito o convite que marcou seu início *offshore* no Brasil. A visão da empresa, de que o mercado brasileiro oferecia fortes oportunidades, se evidenciou nos investimentos imediatos em recursos humanos locais. Hoje a DNV opera no Brasil com um quadro técnico composto totalmente por brasileiros.

De 1974 até os dias de hoje, a DNV Brasil passou por grandes mudanças. As duas pequenas salas que alugava inicialmente deram lugar a dois andares próprios, localizados no centro da cidade do Rio de Janeiro, sede para suas operações na América do Sul. Além disso, foram criados outros oito escritórios localizados em São Paulo, Santos, Caxias do Sul, Belo Horizonte, Fortaleza, Vitória, Salvador e Curitiba. Com essa malha, a DNV Brasil é capaz de oferecer a seus clientes um atendimento rápido, com custo reduzido, quer o serviço requerido esteja relacionado à atividade naval, *offshore* ou industrial.

A descoberta de petróleo em águas territoriais brasileiras deu início a uma série de investimentos por parte da Petrobras, visando desenvolver facilidades para sua extração. O empreendimento que marcou o início da DNV Brasil foi a certificação das três plataformas de concreto, as primeiras construídas no Brasil, destinadas a operar nos poços de Ubarana, no Rio Grande do Norte. Em seguida surgiram os projetos relacionados com a Bacia de Campos e das seis grandes plataformas fixas, em estrutura metálica, construídas para operar na região a DNV certificou quatro: Garoupa, Cherne I, Cherne II e Pampo. Outros dois empreendimentos passíveis de destaque foram a certificação das plataformas de Curimã e a certificação das plataformas chamadas de Família I, estruturas consideradas estratégicas, destinadas a operar em águas rasas. Tudo isso garantiu, na época, uma participação da DNV em 80% do mercado *offshore*.

Nos anos 80, a DNV passou por um período de reestruturação de pessoal, uma vez que acontecimentos internacionais forçaram o corte de investimentos no setor de petróleo, seu carro-chefe na época. Foi também quando o Brasil viveu seu grande período como construtor de navios, chegando a ocupar o segundo lugar no ranking mundial nessa atividade (DNV, 2003). Nesse período, a DNV classificou cerca de vinte e cinco embarcações aqui construídas, envolvendo-se com todos os estaleiros que operavam na época. A DNV destaca com orgulho o fato de ter sido a classificadora dos dois maiores navios mínero-petroleiros já construídos no Brasil: Docefjord e Tijuca.

A década de 90 é considerada a era industrial da DNV Brasil. O mercado internacional começou a sentir os primeiros efeitos da chamada globalização, e a aplicação de sistemas de Gestão da Qualidade, com base nas normas da série ISO 9000, tomou conta da indústria brasileira. A maneira da DNV atuar, tanto na certificação de estruturas *offshore*, quanto na classificação de navios, sempre foi pautada na avaliação de conformidade. Essa experiência secular permitiu que a DNV desenvolvesse, sem maiores dificuldades, sua atividade como certificadora de Sistemas de Gestão, tanto da Qualidade (ISO série 9000), quanto Ambiental (ISO 14001).

Além de se envolver com a certificação de Sistemas de Gestão da Qualidade e Ambiental, a DNV passou a atuar também nas certificações com base na BS 8800 (segurança) e em normas exigidas para os fornecedores de peças para as fábricas de automóveis (QS 9000) e, mais recentemente, na BS 7799 de segurança de informações.

Sem dúvida, a Fase Industrial da DNV Brasil consolidou definitivamente sua atuação no país, aumentando consideravelmente sua gama de clientes. Com mais de mil certificados emitidos no mercado brasileiro, o nome DNV é facilmente identificado e reconhecido.

A DNV enfatiza que o uso de normas nas organizações, mais que uma obrigatoriedade, é decisivo para o desenvolvimento do negócio, reduzindo perdas e desperdícios, ocasionando melhora em resultados financeiros e na performance geral da empresa. Para nortear os seus colaboradores, a DNV define para seu negócio as seguintes diretrizes:

OBJETIVO: Salvaguardar a vida, a propriedade e o meio ambiente.

VISÃO: Ser a primeira escolha dos clientes em tudo o que fazemos.

VALORES:

a) Nós nos preocupamos com os nossos clientes e provemos soluções para melhorar os seus negócios.

b) Nós criamos um ambiente de trabalho onde as pessoas são encorajadas a fazer o seu melhor.

c) Nós adquirimos e dividimos conhecimento e aplicamos para aumentar o valor para os nossos clientes.

d) Nós construímos nosso futuro através de operações lucrativas, inovação e novas oportunidades de negócios.

e) Nós nunca comprometemos a qualidade ou a nossa integridade.

f) Nós obtemos sucesso através da aplicação dos nossos valores.

A segurança da informação é importante para a DNV, porque a empresa depende dos sistemas de processamento de dados nas operações diárias e, à medida que essa dependência aumenta, também o faz a importância da segurança da informação. Além disso, a DNV é sinônimo de confiança e segurança, uma reputação conquistada e fortalecida no dia-a-dia nas interações com os clientes da DNV ao redor do mundo. Portanto, também vê a segurança da informação como um facilitador dos negócios e uma chave para a salvaguarda da reputação

da DNV no mercado e junto ao grande público. Uma abordagem sistemática na proteção dos recursos de informação das ameaças existentes e emergentes é crucial.

Com o surgimento da BS 7799 em 1995, na Inglaterra, por solicitação do Ministério de Indústrias e Comércio inglês, que percebeu a necessidade de proteger a informação que era utilizada nos negócios entre as empresas, algumas organizações uniram-se para criar e divulgar uma diretriz a respeito de boas práticas de gerenciamento para a segurança de informações e a DNV fazia parte desse grupo. Surgia então a primeira versão da BS 7799, norma que posteriormente seria dividida em duas partes, a primeira parte define as boas práticas de gerenciamento de segurança de informações, ou seja, recomendações de como aplicar uma série de controles constantes na própria norma. A segunda parte trata dos requisitos para a implementação e certificação do Sistema de Gerenciamento de Segurança de Informações e possui um anexo que referencia uma lista de controles que pode ser aplicada a uma empresa, e é exatamente essa lista que consta na parte 1 da BS 7799 acrescida de explicações de como e quais alternativas (melhores práticas) a empresa tem para implantar tais controles.

O atual formato do conjunto BS 7799 se deve a algumas revisões que as partes sofreram; atualmente a situação de revisão do conjunto é a seguinte:

a) A parte 1 foi transformada na Norma ISO 17799 no ano de 2000 e foi traduzida pela Associação Brasileira de Normas Técnicas – ABNT em agosto de 2001;

b) A parte 2 continua como BS 7799, passou por uma revisão em setembro de 2002, não possui tradução no Brasil e tem previsão de ser transformada em norma ISO no final do ano de 2004.

A DNV, percebendo a importância do assunto segurança de informações, procurou habilitar-se para a realização de auditorias em Sistemas de Gestão de Segurança de Informações com base na BS 7799, qualificando seu quadro de auditores e procurando divulgar o assunto aos seus clientes e parceiros.

Atualmente nos quadros de auditores da DNV em todo o mundo existem 26 auditores habilitados para a realização de auditorias em BS 7799. Esses profissionais estão classificados por níveis, ou seja, auditores lideres (7) que podem conduzir e atestar uma certificação, auditores (4) que participam da equipe de auditoria, porém ainda sem a quantidade de dias

necessária para comandar a equipe, e auditores interinos (15) que participam também das auditorias, porém igualmente não possuem a quantidade de dias de auditoria necessária para tornarem-se auditores e posteriormente auditores líderes.

A perspectiva e vantagem para esses auditores está no crescimento da demanda das empresas em busca da certificação em BS 7799, o que possibilita aos profissionais realizar uma quantidade maior de auditorias. Conseqüentemente permite a evolução na escala hierárquica de auditores; outra vantagem é o aprimoramento do conhecimento dos auditores em virtude das diferentes soluções implementadas pelas empresas que buscam e alcançam a certificação.

E porque a DNV acredita na eficácia de um Sistema de Gestão de Segurança de Informações é que ela adotou esse padrão baseado na BS 7799 para nortear a sua forma de tratar a informação no seu negócio. Prova disso é a Política de Segurança de Informações descrita a seguir:

> Protegermos os interesses de nossos clientes, funcionários e da DNV, de danos provenientes da perda, mau uso, divulgação não intencional e indisponibilidade dos dados.
>
> Nós iremos:
>
> Estabelecer um nível de proteção para a informação e seus sistemas, proporcional ao valor (tangível e intangível) do recurso de informação;
>
> Proteger a informação da modificação não autorizada, acesso e divulgação não intencional, arquivada ou em transito;
>
> Evitar o uso não autorizado da infraestrutura, serviços de TI e software da DNV;
>
> Impedir a disseminação interna e externa de código malicioso e vírus;
>
> Assegurar que os sistemas da DNV sejam projetados, desenvolvidos, gerenciados e usados de forma segura e eticamente responsável;
>
> Assegurar que os papéis, responsabilidades e autoridades individuais sejam claramente comunicados e compreendidos por todos;
>
> Assegurar o monitoramento da segurança da informação da performance e eficácia do Sistema de Gerenciamento de Segurança da Informação.

A política foi divulgada para todos os colaboradores da DNV de todos os níveis hierárquicos dentro da organização, sendo que a intenção é que todos conheçam essa diretriz e a respeitem, para que dessa forma os ativos e o negócio da empresa sejam preservados e perdurem.

A descrição da metodologia aplicada para a realização do estudo de caso, do cenário onde foi realizado tal estudo, bem como da relevância desse assunto para a empresa e a seus profissionais, foram os objetivos deste capítulo.

CAPÍTULO 5

5 ESTUDO DE CASO – PROCESSO DE AUDITORIA EM BS 7799

O objetivo deste capítulo é apresentar os procedimentos padrão adotados pela DNV em nível mundial, sendo então descritas as recomendações contidas em cada um desses procedimentos, considerando todas as etapas do processo de certificação, desde a cotação do serviço até as auditorias de manutenção do Sistema de Gerenciamento de Segurança de Informações.

5.1 SEQÜÊNCIA DO PROCESSO DE AUDITORIA

O processo de certificação de um Sistema de Gestão de Segurança de Informações é composto de algumas etapas, para cada uma das quais há um procedimento padrão respectivo que serve para orientar a execução da atividade relacionada. As principais etapas do processo são apresentadas na Figura 6.

Fonte: DNV – Marketing BS 7799

Figura 6 Etapas do processo de certificação

O processo de pré-estudo/implementação é realizado pelo cliente e/ou pela consultoria contratada pelo mesmo para implantar e adaptar o Sistema de Gestão de Segurança de Informações na organização dele. A DNV não atua nessa etapa do processo. Após o cliente considerar o seu SGSI implantado é que a DNV começa a sua atuação com a participação da área comercial no levantamento das informações necessárias para elaboração de proposta comercial que irá nortear as condições do negócio entre a DNV e seu cliente.

A participação dos auditores, na fase operacional junto ao cliente, inicia com a realização da pré-auditoria, etapa que tem por objetivo um contato inicial com a empresa, documentação, com os colaboradores e serve para posicionar o cliente em relação ao seu SGSI quanto ao grau de adesão à Norma BS 7799 parte 2, ou seja, uma auditoria com a finalidade de levantar eventuais falhas que ainda existam no SGSI do cliente antes da auditoria inicial.

A auditoria inicial avalia o grau de conformidade do SGSI do cliente e se este estiver satisfatório será então emitido certificado com validade de três anos.

Auditorias de *Follow Up* têm por objetivo avaliar as ações corretivas propostas pelos clientes para sanar não-conformidades identificadas como graves, ocorrem se existirem não-conformidades graves em auditorias iniciais, de manutenção ou re-certificação.

Auditorias periódicas ocorrem conforme a freqüência estipulada em contrato, com o objetivo de avaliar a continuidade da implementação do SGSI do cliente.

Essas etapas e outras, que suportam essas atividades, têm procedimentos que estão citados nas próximas seções.

5.1.1 ***Procedimento de Cotação e Revisão de Cotação***

Quando o departamento comercial da DNV é contatado por um possível cliente, deve-se utilizar esse procedimento como base para a elaboração da proposta comercial que irá definir os critérios da prestação de serviço (auditoria em BS 7799), que será realizada nesse cliente. Os seguintes pontos devem ser considerados quando da preparação da cotação:

a) localização exata (geograficamente, área industrial, residencial, misturada);

b) número de unidades com atividades de negócio, incluindo unidades de recuperação de desastre, as atividades realizadas em cada unidade e o número de empregados de cada uma dessas unidades (ativos da empresa);

c) o nível dos controles de segurança requeridos para o negócio ou pelos clientes, por exemplo, militares, privacidade pessoal, confidencialidade comercial (controles);

d) processos que tenham um escopo com atividades fora das instalações, por exemplo, premissas de clientes ou premissas para recuperação de desastres (plano de continuidade de negócios);

e) maior característica da tecnologia de informação em uso, inclusive os requisitos adicionais de contratos específicos ou referências a documentos aplicáveis à organização;

f) maior serviço de processamento da informação para cada tipo de usuário, por exemplo, pessoal, financeiro, vendas incluindo clientes e fornecedores (se aplicável), considerando o número de usuários de cada área;

g) a posição dos grupos diretamente responsáveis por administrar e gerenciar a segurança (definição da política, escrita dos procedimentos, segurança da unidade, administrar sistemas, proteção de vírus, incidentes de segurança, proteção de dados);

h) produtos e ferramentas de segurança em uso (controle de acesso à unidade, crachás, controle de acesso à sistema de TI, controle de vírus, monitoramento de ambiente, *backup*);

i) descrição genérica da estrutura da documentação do Sistema de Gerenciamento de Segurança de Informações (política, manual de segurança, instruções de trabalho);

j) descrição genérica do método de análise de risco utilizado para identificar e avaliar o risco;

k) declaração de aplicabilidade, ou documento equivalente, com a identificação dos controles da BS 7799 que são aplicáveis;

l) cópia da certificação ISO 9001 aplicável à organização (se for aplicável);

m) *check list* dos anexos para aplicação;

n) descrição do sistema de segurança;

o) relatório de análise de risco;

p) declaração de aplicabilidade;

q) certificado ISO 9000 ou outro.

5.1.1.1 Estimativa de Tempo para a Auditoria e/ou Pré-Auditoria

A estimativa de tempo para certificação em BS 7799 segue o mesmo rateio de dias e características de estrutura da certificação ISO 9000. Para isso deve-se utilizar um guia para estimativa de homens-dia que está definida nas Figuras 7, 8 e 9. Esse contexto considera o fato que a BS 7799 é normalmente mais complexa de auditar, à medida que o negócio da empresa também pode ficar mais complexo.

Essa estimativa de tempo pode ser ajustada pelos escritórios da DNV à medida que a experiência com a execução do serviço for adquirida e por conseqüência o ajuste desse procedimento.

Quando um cliente deseja aplicar-se à certificação BS 7799 e ISO 9000, ou já for certificado ISO 9000, a cotação deve considerar auditorias conjuntas. Isso possibilitará uma redução na carga da auditoria, pois existem situações comuns a serem verificadas, tais como política, procedimentos documentados, manutenção de registros. Tal redução deve considerar a realização de visitas conjuntas, e um método simples para determinar o tempo a ser reduzido é o seguinte: um dia de trabalho para auditorias que tiverem cotação acima de seis homens-dia, meio-dia de trabalho para aquelas cotações de três a seis homens-dia, e para cotações abaixo de três homens-dia nenhum dia de trabalho pode efetivamente ser reduzido.

5.1.1.2 Definição da Carga da Auditoria

A Figura 7 é utilizada para definir o grau de complexidade das atividades de um negócio *versus* estrutura da Tecnologia da Informação em uma determinada empresa, dessa maneira os critérios de classificação são: alta, que tem como característica a diversidade de atividades (muitas delas críticas para a empresa), unidades e ou filiais, colaboradores e atendimento de requisitos legais especiais, bem como aplicações não padronizadas em vários

tipos de plataforma, interações de sistemas de informações críticos ou que processam informações sensíveis. A classificação média, para empresas que possuem tamanho médio, com pouca diversidade de atividades, com conexão externa fixa, com desenvolvimento de aplicativos próprios. E por fim, a classificação baixa, para aquelas empresas pequenas com atividades restritas, poucos colaboradores, sem requisitos legais específicos, com aplicações padrões em uma única plataforma e redes locais simples.

Categoria				Fatores de Impacto (Atividade do Negócio/Estrutura da Organização)
A				Grupo de tamanho médio a grande/companhia/unidades com atividades que incluem muitas funções, ou seja, P &D, Desenvolvimento, produção e/ou construção, serviços. Negócios em muitas localidades. Um número de cooperadores/parceiros. Eventualmente negócios em vários países. Requisitos legais especiais.
	M			Companhia de tamanho pequeno a médio/unidades com 1 ou 2 áreas de negócio incluindo P&D, desenvolvimento, produção e/ou construção, serviços.
		B		Companhias de média a grande com produção e/ou construção com atividades limitadas, incluindo desenvolvimento. Um único país e um número limitado de cooperadores/parceiros, eventualmente algum requisito legal específico.
				Companhias de pequena a média/unidade com produção e/ou construção com atividade limitada incluindo desenvolvimento.
				Companhia de pequena a média/unidade com instalação /serviço/vendas. Negócio principal em único local, único ou poucos cooperadores/parceiros – nenhum requisito legal específico.
Categoria				Estrutura de IT
A				Muitas "*extra-nets*" conectadas. Um número de aplicações não padronizadas em vários tipos de plataforma. Interação potencial sistemas de informações críticos ou sistemas de informação que processam informações sensíveis.
	M			Conexão externa fixa. Compartilhamento de instalações (por exemplo, computadores, sistemas de telecomunicações, etc.) com outros. Complexidade dos sistemas de informação. Desenvolvimento de *software* aplicativo próprio utilizado na organização.
		B		Única ou várias "*LAN's*" conectadas. Conexão com Internet (*ISDN, Broadband*, etc.) e *WEB-site* de informações para clientes. Única aplicação padrão em uma única plataforma.
				Rede local simples com alguns computadores pessoais e/ou estações de trabalho. *E-mail* utilizado via Internet através de acesso discado.
				Sem rede – um computador pessoal ou uma rede local simples com algumas estações de trabalho. Sem conexões externas.

Fonte: Procedimento DNV – Anexo A

Figura 7 Avaliação da complexidade para definição da carga de auditoria

5.1.1.3 Estimativa dos Fatores Impactantes x Estrutura de TI

A Figura 8 define, pelo resultado da categoria de fatores impactantes versus estrutura de TI, a faixa de dias necessária para a realização do processo de auditoria em empresas.

Fatores Impactantes/ Estrutura de TI	Baixa (Homens-dia)	Média (Homens-dia)	Alta (Homens-dia)
Baixa	3-4	5-7	7-10
Média	4-5	6-10	8-14
Alta	5-6	7-12	9-18

Fonte: Procedimento DNV – Anexo A

Figura 8 Estimativa dos fatores impactantes

5.1.1.4 Estimativa de Homens-Dia para Certificação do SSGI

A Figura 9 mostra a distribuição acima estimada de homens-dia para a atividade de certificação.

Fatores Impactantes/ Estrutura de IT	Pré-Auditoria	Certificação				Manutenção da Certificação (por ano)
		Revisão da Documentação	Auditoria Inicial Passo 1	Auditoria Inicial Passo 2	Estimativa Total para Certificação	
Baixo–Baixo	1-4	1	1	1-2	3-4	1-2
Baixo–Médio	1-7	1-2	2	2-3	5-7	2-4
Baixo–Alto	2-10	2	2-3	3-5	7-10	3-6
Médio–Baixo	1-5	1	1-2	2	4-5	2-4
Médio–Médio	1-10	1-2	2-3	3-5	6-10	3-6
Médio–Alto	2-14	2	2-3	4-9	8-14	4-8
Alto–Baixo	1-6	1	2	2-3	5-6	2-4
Alto–Médio	1-12	1-2	2-3	4-7	7-12	3-7
Alto–Alto	2-18	2-3	3-4	4-11	9-18	4-10

Fonte: Procedimento DNV – Anexo A

Figura 9 Estimativa de homens-dia

Nota: Auditoria Inicial – passo 1 consiste na visita inicial e na revisão do sistema técnico. Considerações especiais sempre devem ser levadas em conta quando da necessidade de um técnico *expert* durante a auditoria. Essa necessidade de um *expert* é baseada na complexidade de TI da organização e no conhecimento do auditor. A quantidade necessária de homens-dia deve ser proporcional à quantidade de múltiplas unidades a serem auditadas.

5.1.1.5 Auditorias Periódicas

As regras sobre a freqüência das auditorias periódicas são as mesmas que as para ISO 9000. Não existem requisitos especiais, então auditorias anuais podem ser oferecidas em casos básicos.

5.1.1.6 Verificação e/ou Certificação em Múltiplas Unidades

A área comercial da DNV deve observar cuidadosamente a decisão para amostragens múltiplas na área do Gerenciamento de Segurança de Informações por ser mais complexa do que a decisão na área de sistemas da qualidade. Os organismos certificadores que desejam utilizar a mesma amostra, baseada na abordagem para verificação em múltiplas unidades, necessitam manter procedimentos que incluam a gama completa das questões que serão apresentadas abaixo nas unidades da amostragem do programa.

O organismo certificador (DNV) deve garantir que a emissão/revisão do contrato inicial identifique na medida do possível a maior diferença entre as unidades tais, que o nível adequado de amostragem seja determinado de acordo com as previsões a seguir.

Onde uma organização possuir um número similar de unidades cobertas por um único Sistema de Gerenciamento de Segurança de Informações, o certificado pode ser emitido para a organização, a fim de considerar todas as unidades de forma a comprovar que:

a) todas as unidades estão operando sob o SGSI, com uma administração centralizada, auditorias e revisão do gerenciamento central;

b) todas as unidades sejam auditadas de acordo com o procedimento de auditoria interna da empresa;

c) um número representativo de unidades deve ser verificado pelo organismo certificador, levando em consideração os requisitos abaixo:

   - resultado das auditorias internas da matriz e das unidades;
   - resultado da revisão gerencial;
   - variação do tamanho das unidades;
   - variação dos negócios das unidades;
   - complexidade do SGSI;

- complexidade do Sistema de Informações das diferentes unidades;
- variação das práticas de trabalho;
- variação das atividades sob o escopo;
- potenciais interações com sistemas de informações críticos ou sistemas de processamento de dados sensíveis;
- requisitos legais diferindo.

d) a amostragem deveria ser em parte seletiva, baseada na variação do tamanho das unidades (ponto c acima) e em parte não seletiva e deveria resultar numa faixa de diferentes unidades inicialmente selecionadas, sem excluir o elemento randômico para seleção das unidades;

e) cada unidade inclusa sob o SGSI e sujeita a ameaças significativas aos ativos, vulnerabilidades ou impactos devem ser auditadas pelo organismo certificador previamente à certificação (análise de risco);

f) o programa de auditoria deve ser determinado à luz dos requisitos citados acima considerando o tempo adequado para cobrir todos as unidades da organização ou o escopo da certificação do SGSI considerado na declaração de aplicabilidade;

g) no caso de uma não-conformidade ser observada para o escritório central e alguma unidade da organização, procedimento para ação corretiva deve ser implementado no escritório central e em todas as unidades cobertas pela certificação.

5.1.1.7 Unidades Compartilhadas

Considerações especiais devem ser tomadas em unidades compartilhadas, isto é, onde várias companhias utilizam as mesmas instalações. Isso é permitido para execução da certificação para um negócio que seja partilhado, sujeito às seguintes condições:

a) a organização deve ser claramente identificada e gerenciar as interfaces com outros negócios/organizações da unidade;

b) a organização deve identificar todos os aspectos relevantes, em conexão com outras atividades na unidade, e que influenciam ou possam influenciar ambos os

objetivos formais (melhoria ou investigação) ou controle operacional (análise de risco).

5.1.1.8 Organizações Prestadoras de Serviço

Onde não for possível definir a localização, a abrangência da certificação deve levar em conta a sede do cliente, bem como a entrega desses serviços. Em casos especiais, a certificação pode ser executada unicamente onde os serviços são entregues ao cliente. Em tais casos, a interface com a sede do cliente deve ser auditada.

Os procedimentos citados abaixo são todos relacionados às atividades operacionais que ocorrem na DNV e estão diretamente ligados às atividades de execução da auditoria e, nesse caso, ao processo de Segurança de Informações baseada na BS 7799.

5.1.2 ***Nomeação e Competência da Equipe Auditora***

Os requisitos abaixo devem ser aplicados à verificação de certificação.

Todos os membros da equipe auditora (cada membro, exceto *expert* técnico) devem estar aptos para demonstrar a apropriada experiência e compreensão de todos os passos a seguir:

a) norma de Gerenciamento de Segurança de Informações ou documento normativo;

b) conceitos gerais de Sistemas de Gerenciamento;

c) questões relacionadas a várias áreas da Segurança de Informações;

d) princípios e processos relacionados à análise de risco e ao gerenciamento de risco;

e) princípios de auditoria.

Quanto à equipe auditora (como um todo), pelo menos um membro da equipe deveria satisfazer as seguintes atividades, segundo os critérios do organismo de certificação assumindo a responsabilidade dentro do time:

a) gerenciar a equipe;

b) conhecer legislação, requisitos regulamentares legais na área específica de segurança de informações;

c) identificar ameaças relacionadas à segurança de informações;

d) identificar vulnerabilidades da organização e compreender o seu impacto, efeito e controle;

e) conhecer o atual estado da arte técnico no setor;

f) conhecer a análise de risco relacionados à segurança de informações.

A equipe auditora deve ser competente para investigar se indicações de incidentes de segurança na organização são tratados nas formas apropriadas e nos elementos do SGSI da organização.

Uma equipe auditora pode consistir de uma pessoa que possa atender a todos os critérios estabelecidos acima.

Experts Técnicos: um *expert* técnico, com conhecimento específico do processo e da legislação sobre segurança de informações emitidas que afetem a organização, mas que não satisfaça todos os critérios acima, pode ser parte integrante da equipe auditora. O *Expert* técnico não deve atuar independentemente.

5.1.3 ***Procedimento de Revisão da Documentação***

A documentação a ser revisada deve ser consistente com no mínimo:

a) documentação e/ou declaração da política;

b) documentação da análise de riscos;

c) declaração de aplicabilidade;

d) documento do escopo do SGSI;

e) estrutura organizacional;

f) descrição da tecnologia incluindo esquema de rede;

g) manual da Política de Segurança que deveria incluir os seguintes (os mesmos citados acima, mas em um único manual);

h) política de segurança, na versão completa e resumida;

i) a natureza da organização corresponde com a sua necessidade de segurança;

j) gerenciamento do ambiente de segurança – como a organização gerencia a segurança;

k) descrição do Sistema de Gerenciamento de Segurança de Informações;

l) procedimentos para operação e manutenção do SGSI;

m) documentação e estrutura de registros com referência ao menor nível da documentação;

n) escopo de segurança, definindo os limites do ambiente de segurança de informações;

o) descrição do sistema de análise de risco;

p) um sumário dos controles e das proteções implementados.

5.1.4 *Procedimento para Visita Inicial*

Para a visita inicial, os seguintes requisitos devem ser considerados:

a) uma avaliação da análise de riscos, especificados no relatório de análise de riscos, devendo ser completo e levar em consideração os produtos e as ferramentas de segurança especificados em uso;

b) a revisão da declaração de aplicabilidade estabelecida;

c) a revisão do nível dos controles de segurança requeridos, tal como especificado pela organização;

d) a revisão das maiores características de tecnologia de informação em uso – incluindo o plano de rede de trabalho;

e) a revisão dos serviços de processamento da informação para cada tipo de usuário;

f) um acordo da natureza da confidencialidade estabelecida, isto é, não deve existir dúvida quanto ao acesso do auditor a registros pessoais, etc., dentro da organização.

Na condução da visita inicial, o auditor líder (responsável pela equipe) deve verificar se todos os auditores terão acesso a todos os registros relevantes e necessários para a verificação efetiva do SGSI.

O auditor-líder deve avaliar a análise de risco do cliente e o meio pelo qual a organização avaliou o seu significado. O objetivo disso é estabelecer se a verificação do risco da organização reflete apropriadamente as suas atividades e a extensão dos limites das suas atividades, tal como definida na norma de SGSI ou no documento normativo.

O auditor-líder deve analisar a declaração de aplicabilidade do cliente. O objetivo é estabelecer uma correta compreensão dos termos definidos, bem como se a declaração de aplicabilidade reflete corretamente o escopo de segurança de informações da organização.

O auditor-líder deve verificar se a documentação do sistema está suficientemente implementada e justifica o próximo passo da auditoria inicial. Além disso, o auditor-líder deve verificar se o sistema é:

a) baseado em uma avaliação de análise de riscos;

b) definido para controlar e melhorar a segurança de informações;

c) capaz de garantir o atendimento à legislação;

d) baseado na declaração de aplicabilidade;

e) baseado em objetivos e metas;

f) auditável.

Credibilidade da auditoria interna: o auditor-líder deve estabelecer se a freqüência das auditorias internas está adequada aos aspectos de segurança de informações. O líder da equipe deve deixar o cliente consciente de alguns passos adicionais que podem ser requisitados para uma verificação mais detalhada durante a auditoria inicial:

a) registros pessoais de natureza confidencial;

b) detalhes de qualquer não-conformidade interna identificada junto com os detalhes das ações corretivas e/ou preventivas tomadas nos últimos 12 meses (ou desde do início da implementação do sistema se esta for menor que 12 meses);

c) revisão dos registros de gerenciamento;

d) registros de qualquer sistema de recebimento de comunicações e qualquer ação tomada para responder a este sistema.

5.1.5 *Procedimento para Auditoria Inicial*

Os objetivos para esse tipo de auditoria são:

a) determinar o que a organização não excluiu do escopo do seu SGSI e quais os elementos da sua operação que deveriam apropriadamente estar sob o seu escopo;

b) garantir que a análise de risco da organização reflita as atividades e a extensão dos limites dessas atividades, assim como definido na norma do SGSI ou documento normativo;

c) confirmar que a análise de risco da organização é reflexo da declaração de aplicabilidade da mesma;

d) garantir que as interfaces com os serviços ou atividades que não são realizadas dentro da organização são completamente conhecidas e tratadas na análise de risco;

e) determinar se a documentação, estabelecida e implementada do SGSI está trabalhando para garantir o atendimento da legislação aplicável;

f) determinar se o SGSI está indo ao encontro dos objetivos e das metas da empresa, respeitando a segurança de informações;

g) determinar se a implementação do SGSI propriamente protege a informação e os ativos computacionais.

A auditoria deve focar no atendimento pelo cliente dos requisitos de segurança de informação citados abaixo:

a) gerenciamento do ambiente de segurança (política, declaração de aplicabilidade, etc.);

b) implementação;

c) documentação;

d) controles documentados;

e) medição dos controles de segurança de informação, que incluem:

- política de segurança;
- segurança organizacional;
- classificação e controle de ativos;
- segurança em pessoal;
- segurança física e ambiental;
- gerenciamento de computadores e redes;
- sistema de controle de acesso;
- sistema de desenvolvimento e manutenção;
- plano de continuidade de negócios;
- conformidade.

A integração do SGSI com qualidade, ambiente ou segurança poderia:

a) ter elementos comuns (documentos, registros, política, etc.) que seriam acessados por qualquer dos auditores-líderes;

b) o auditor-líder do SGSI poderia ter tempo para verificar a sua respectiva parte.

Áreas críticas, tais como medição dos controles de segurança de informação, devem ser auditadas pelo auditor-líder do SGSI (com assistência possível de um auditor qualificado em SGSI ou especialista).

5.1.6 *Procedimento para Auditorias Periódicas*

Auditorias periódicas devem ser agendadas e executadas de acordo com a Norma ISO 19011 (norma que especifica o processo de auditorias). O plano de auditorias periódicas, elaborado ao final da visita inicial, deve demonstrar que todos os requisitos relevantes serão revisados durante os três anos do ciclo.

Controles que devem ser revisados a cada visita incluem:

a) auditorias do sistema operacional;

b) tratamento de reclamações;

c) tratamento dos incidentes de segurança;

d) condução das revisões de segurança;

e) uso adequado do certificado e dos logotipos.

Visitas adicionais podem ser requisitadas quando mudanças significativas na certificação da organização ocorrerem ou a sua abordagem para gerenciamento da segurança mudar, ou no caso de falha da implementação satisfatória da correção de não-conformidades.

A certificação da BS 7799 requer que a cada três anos uma auditoria de recertificação seja executada. A auditoria de recertificação deve ser planejada com base nas auditorias periódicas anteriores. O plano deve prever como serão cobertos os mesmo itens da certificação inicial, incluindo a verificação dos produtos do cliente, serviços e mercados se ainda continuam consistentes com a declaração de aplicabilidade e conseqüentemente com o Sistema de Gerenciamento de Segurança de Informações.

5.1.7 *Não-Conformidades e Acompanhamento de Ações Corretivas*

Além das não-conformidades do procedimento genérico da DNV, devem ser consideradas as seguintes situações:

a) a falta de evidência documentada da realização da Análise de Risco;

b) falta ou inadequação de um plano de continuidade de negócios;

c) ambigüidades, falta de clareza, falta de equilíbrio, falta de acuracidade, fatos dúbios de informações ou falta de representação na declaração de aplicabilidade;

d) discrepância entre a informação da declaração de aplicabilidade e a verificação da informação no local.

5.1.8 *Procedimento para Definição do Escopo do SGSI*

As organizações devem definir os escopos dos seus Sistemas de Gerenciamento de Segurança de Informações. A regra do organismo certificador é evidenciar consistência e

garantir que a organização não excluiu do seu escopo elementos do SGSI e, das suas operações, itens que deveriam estar sob esse escopo.

Organismos certificadores devem garantir que a análise de risco da organização reflete apropriadamente as suas atividades e extensão dos limites dessas atividades, definidas na Norma de SGSI ou em documento normativo. Organismos certificadores devem confirmar se isso está refletido na declaração de aplicabilidade da organização.

Interfaces com serviços ou atividades, que não são executadas sob o escopo do SGSI, devem ser identificadas dentro do SGSI objeto da certificação (por exemplo, elas devem constar da análise de risco).

Em acréscimo à definição da atividade da empresa, o escopo deve definir quais os locais ou partes de algum local serão cobertas pelo certificado.

As atividades do cliente devem ser identificadas com termos genéricos para descrever a sua atividade principal. Isso deve estar claro quanto à extensão da responsabilidade de gerenciamento, por exemplo, em relação a companhias que compartilham um mesmo local com outra empresa.

Isso também deve ficar claro se alguma atividade importante for excluída, tais como *warehousing* ou vendas e marketing.

Em resumo, no escopo da certificação, deve-se demonstrar:

a) a identificação dos locais;

b) as atividades principais;

c) as exclusões.

5.2 PROCESSO DE CERTIFICAÇÃO

O objetivo desta seção é apresentar os resultados da aplicação dos padrões internacionais definidos na seção anterior em um processo de auditoria, em uma empresa nacional, bem como os resultados da aplicação da metodologia utilizada.

A primeira etapa no processo de certificação foi a prospecção e elaboração da proposta para certificação do cliente. Essa etapa seguiu o procedimento de cotação e revisão de cotação apresentado no capítulo anterior. Para coleta dos dados necessários do cliente, foi utilizado um formulário para elaboração de proposta (anexo B), que permite obter informações básicas e detalhadas para a área de Segurança de Informações e, assim, elaborar a proposta de serviço.

Com a resposta por parte do cliente, foi possível obter a informação inicial sobre número de funcionários, unidades envolvidas e escopo inicial no qual a empresa estava se aplicando para a certificação. Isso possibilitou à DNV consultar as tabelas para estimativa do impacto de fatores versus estrutura de TI, estimativa homens-dia e a de distribuição desses homens-dia por etapa do processo de auditoria, elaborando a proposta para certificação da organização.

Nessa etapa pode ser necessário revisar a proposta em virtude da concorrência e do ajuste de alguma informação que o cliente eventualmente pode não ter informado. Porém, é importante ressaltar que o número mínimo de homens-dia estipulado no procedimento deve sempre ser seguido, sob pena da própria DNV ser notificada por não atender às regras estipuladas pelos acreditadores do processo de certificação.

É da informação da proposta que o auditor-líder poderá elaborar a programação para a visita inicial, determinando o escopo da certificação e o tempo para as verificações, bem como já terá uma idéia sobre as atividades da empresa em questão, podendo até mesmo solicitar alguma documentação prévia antes de efetivar a visita ao local propriamente dito. Importante ressaltar que essa programação é tentativa, pois a visita inicial será o primeiro contato que a equipe auditora terá com o cliente da DNV.

De posse da proposta é que o pessoal de apoio da DNV também poderá selecionar a equipe auditora com base nas qualificações dos seus profissionais e também comparando com as atividades do cliente em questão. Atualmente, no Brasil não existem auditores qualificados para atender à certificação de Segurança de Informações, sendo um profissional da DNV da Inglaterra o responsável pelas atividades de verificação do cliente da DNV em estudo. Tal profissional atendia aos requisitos especificados no procedimento de nomeação de competência da equipe auditora citada na seção anterior.

O processo de visita inicial foi previsto para a realização em três dias, pois a empresa havia informado um tipo de atividade e escopo que, em princípio, previa que o Sistema de

Gerenciamento de Segurança de Informações cobriria todas as unidades. Quando da realização da visita inicial, foi identificado que a atividade a ser coberta seria apenas na unidade principal e não envolveria as demais unidades, reduzindo assim o número de funcionários envolvidos e as atividades a serem cobertas. Assim, foi revisada a proposta para que, na etapa seguinte, apenas dois dias de verificação seriam realizados na auditoria inicial. Na visita inicial, também foi possível ajustar o escopo para a nova situação e conhecer a documentação exigida: a política de segurança, análise de risco, declaração de aplicabilidade, plano de continuidade de negócio e características da tecnologia de informação utilizada pelo cliente. É nessa etapa que a equipe auditora deve procurar avaliar a documentação definida, entender o negócio da organização e verificar o grau de conformidade dessa documentação com os requisitos da norma BS 7799, parte 2.

Como resultado da visita inicial, o auditor-líder gera um relatório com todas as observações efetuadas pela equipe auditora a respeito dos requisitos do Sistema de Gerenciamento de Segurança de Informações que não estavam atendendo a contento as definições da norma. Com base nesse relatório, a organização deve providenciar as ações necessárias para correção ou melhoria do seu SGSI antes da etapa seguinte, que é a auditoria de certificação, também conhecida como auditoria inicial.

O processo da auditoria inicial foi executado em dois dias, sendo revisada a documentação da empresa e verificada a implementação do Sistema de Gerenciamento de Segurança de Informações em comparação com a Norma BS 7799 e os controles determinados pela empresa. Importante ressaltar que o cliente já era certificado em ISO 9001, o que facilitou a verificação da documentação, pois já existia uma estrutura pré definida para a qualidade que pôde ser amplamente utilizada. Além disso, o pessoal da empresa também já estava ambientado com o processo de auditoria. Apesar disso, a organização optou por não realizar auditoria integrada (ISO 9001 e BS 7799 juntas) nesse momento.

O início dessa etapa é executado com o envio do programa de auditoria para a organização, agora com o escopo definido, com as áreas especificadas e com o tempo ajustado para verificar cada uma delas. É importante ressaltar que, mesmo assim, o programa continua sendo considerado experimental, pois ajustes posteriores poderão ser realizados. Quando do envio da programação, o cliente tem um prazo para manifestar-se, sugerindo algum tipo de modificação. Caso isso não ocorra, o auditor-líder considerará a agenda como aprovada.

O objetivo do auditor-líder, na auditoria inicial, é avaliar se o Sistema de Gestão de Segurança de Informações que foi documentado está de fato implementado e sendo executado em todas as áreas/atividades previstas no escopo da certificação. Além disso, a equipe auditora tem que avaliar se as pessoas entrevistadas demonstram que conhecem o funcionamento desse sistema, ou seja, a tarefa da equipe auditora é constatar a conformidade em relação à prática *versus* documentação *versus* norma BS 7799.

Nessa etapa de auditoria inicial, foram entrevistadas praticamente todas as pessoas envolvidas com o escopo da certificação, desde a diretoria até a função operacional mais simples da hierarquia da empresa. Importante destacar que o processo de verificação de uma auditoria sempre é por amostragem, no sentido de escolher as pessoas a entrevistar e aqueles processos que podem ter várias atividades inclusas.

Como resultado dessa etapa, a equipe gera, ao final da auditoria, um relatório que contém todas as não-conformidades (evidência do não-atendimento da norma) ou observações (possíveis não-conformidades) que foram identificadas ao longo do processo. É comum na DNV ser realizada, ao final do dia, uma reunião com o cliente para informá-lo dos resultados. Isso possibilita ao cliente manter-se atualizado sobre o andamento dos trabalhos e também permite à organização providenciar ações corretivas ainda durante a auditoria, se possível.

O resultado da auditoria foi satisfatório, apesar de terem sido efetuados registros de não-conformidades, porém nenhum que impedisse a DNV de recomendar a empresa para a certificação do seu SGSI com base na BS 7799, parte 2.

Como etapas a serem atendidas no futuro, as auditorias de manutenção serão anuais e verificarão todos os principais itens do SGSI da empresa, e essa verificação deverá ocorrer em setembro de cada ano, até o encerramento dos três anos de validade do certificado. Passados esses três anos, a empresa pode então continuar com o processo realizando uma auditoria de recertificação, que habilitará a empresa a continuar com a certificação por um período de mais três anos e assim sucessivamente se esta o desejar.

A Figura 10 apresenta os passos do processo de auditoria, discriminando-se cada etapa realizada, os procedimentos correlatos utilizados e os resultados obtidos, bem como eventuais situações de modificação citados no capítulo 6.

Descrição do Processo	Procedimento Seguido	Resultado Obtido	Observações (ver cap.6)
1 – Envio do Formulário para o Cliente	Procedimentos de Cotação e Revisão de Cotação	Obtenção dos Dados do Cliente para Elaboração da Proposta (ver anexo B)	
2 – Preparação da Proposta	Procedimentos de Cotação e Revisão de Cotação	Definição da Carga de Auditoria e Valores	Revisão das informações por auditor qualificado
3 – Definição do Escopo	Procedimento para Definição do Escopo do SGSI	Definição da abrangência do SGSI	
4 – Aceite do Cliente	Procedimentos de Cotação e Revisão de Cotação	Confirmação das Informações citadas na Proposta	
5 – Avaliação e Definição da Equipe Auditora	Procedimento de Nomeação e Competência da Equipe Auditora	Profissionais selecionados de acordo com a necessidade da avaliação a ser realizada	
6 – Agendamento da Auditoria	Procedimento para Visita Inicial	Envio do Programa para o Cliente, especificando equipe auditora, horários da auditoria e logística necessária	
7 – Realização da Revisão da Documentação e Visita Inicial	Procedimento de Revisão da Documentação e Procedimento para Visita Inicial	Primeiro contato direto da equipe auditora com o cliente	Concentrar esforços na revisão da documentação e identificação do negócio das organizações
8 – Geração do Relatório da Auditoria	Procedimento de Revisão da Documentação e Procedimento para Visita Inicial	Registro dos pontos identificados como possíveis desvios de atendimento da Norma	
9 – Ajuste do Escopo	Procedimento para Definição do Escopo do SGSI	Adequação da definição da abrangência do SGSI	
10 – Ajuste da Carga de Auditoria	Procedimento de Cotação e Revisão de Cotação	Adequação do número de dias-homem necessários para a auditoria de certificação	
11 – Agendamento da Auditoria Inicial	Procedimento para Auditoria Inicial	Envio do Programa para o Cliente, especificando equipe auditora, horários da auditoria e logística necessária	
12 – Realização da Auditoria de Certificação	Procedimento para Auditoria Inicial	Verificação do SGSI do Cliente	
13 – Emissão dos Registros da Auditoria	Procedimento para Auditoria Inicial	Emissão do Relatório da Auditoria; dos registros de Não-Conformidade; do Plano de Auditorias Periódicas; da recomendação para certificação	
14 – Agendamento da Auditoria Periódica Obs. 1: (repete-se tantas vezes quantas forem definidas no contrato, ao longo de três anos)	Procedimento para Auditorias Periódicas	Envio do Programa para o Cliente, especificando equipe auditora, horários da auditoria e logística necessária	
15 – Realização da Auditoria Periódica (Obs. 1)	Procedimento para Auditorias Periódicas	Verificação dos Processos marcados no Plano de Auditorias Periódicas	Obs1: etapa realizada "n" vezes de acordo com contrato.
16 – Emissão dos Registros de Auditoria (Obs. 1)	Procedimento para Auditorias Periódicas	Emissão do Relatório e possíveis Não-conformidades	

Fonte: Compilação dos Procedimentos DNV – Anexo A

Figura 10 Passos do processo de auditoria no mercado nacional

Como resultado da aplicação dos procedimentos pode-se citar que existem fatores que facilitam a aplicação dos procedimentos e fatores que dificultam essa aplicação. Sob a ótica do cliente, o aspecto que funcionou como facilitador é o conhecimento que o mesmo possui do seu Sistema de Gestão de Segurança da Informação. A respeito das dificuldades do cliente, foi percebido que a identificação dos ativos envolvidos no SGSI, a definição do escopo desse SGSI, a legislação aplicável e a expectativa da realização da própria auditoria foram os aspectos que contribuíram de forma negativa no processo da auditoria.

Sob a ótica da equipe auditora, os aspectos que funcionaram como facilitadores foi a documentação do SGSI, o conhecimento do pessoal envolvido e a utilização dos relatórios padrão da DNV. Em relação às dificuldades percebidas pela equipe auditora, as principais foram: a identificação das atividades a serem cobertas pelo Sistema de Gestão de Segurança de Informações, a definição da carga de auditoria a ser realizada e a legislação aplicável ao negócio da empresa. O detalhamento a respeito da aplicação desses procedimentos pode ser verificado no capítulo 6.

Em relação à metodologia aplicada o que se pode constatar é que a fase da coleta de dados foi executada sem problemas, pois a habilidade para entrevistar e obter as informações adequadas (requisito atendido na qualificação dos auditores) e a facilidade de poder utilizar questionários (formulários) previamente elaborados permitiram executar esta etapa satisfatoriamente, importante ressaltar que na sua maioria estes documentos são os relatórios utilizados no processo da auditoria e conseqüentemente de natureza confidencial.

O que exige um pouco de atenção e sensibilidade por parte do entrevistador é o estado de ansiedade dos entrevistados, devido a natureza do processo da auditoria, o entrevistado pode ter dificuldade em repassar informações devido ao nervosismo. Outro fator importante é a amostragem de entrevistas a ser realizada, como no processo de auditoria não se exige um número mínimo ou máximo de amostras, o entrevistador deve ter cuidado com as evidências a serem coletadas, pois estas é que determinarão o número de amostras a serem realizadas, ou seja, se o entrevistador conseguir através de evidências comprovar que o assunto que esta sendo avaliado está conforme a norma ele pode decidir por encerrar a amostra com uma única entrevista ou estender a coleta de dados e levantamento de evidências com outros entrevistados.

Em relação a etapa de coleta de evidências, o que se pode perceber é o cuidado que o entrevistador deve ter em buscar analisar um gama variada de evidências (documentos, registros, entrevistas, observação de uma atividade) uma vez que essas evidências é que vão indicar ao entrevistador o momento de prosseguir ou encerrar a coleta das mesmas. Nesta etapa o treinamento do entrevistador é fundamental, pois no mesmo tempo que deve coletar as evidências ele também deverá analisar se essas evidências atendem ao padrão utilizado como referência, e na mesma lógica que na etapa anterior, o que vai determina se o entrevistador prossegue com a coleta de evidências é o resultado da análise dos exemplos (documentos, registros, entrevistas, atividade) avaliados.

A etapa da análise de evidências torna-se fundamental para sustentar todo o processo de pesquisa, uma vez que é do resultado desta análise que se determina a necessidade de realizar novas coletas de dados e evidências. O que provavelmente se diferencia em relação ao método usual de análise de evidências, é que esta atividade é realizada geralmente no mesmo momento que se realizam a coleta de dados e evidências, pois desta forma o entrevistador poderá decidir se deve aumentar a amostragem ou não.

A geração do relatório respeitou a utilização de formulários previamente definidos no modelo proposto na empresa estudada (relatório de auditoria), o que permitiu expor de forma clara e objetiva as informações coletadas, analisadas e as conclusões resultantes da atividade da auditoria. Como forma apresentação dos resultados da pesquisa a geração do relatório mostrou-se adequada aos propósitos.

Os objetivos deste capítulo foram de apresentar os padrões internacionais utilizados para a definição da execução da atividade de verificação de um Sistema de Gerenciamento de Segurança de Informações em um determinado cliente da DNV, bem como os resultados dessa utilização.

CAPÍTULO 6

6 CONCLUSÕES

O objetivo deste trabalho foi descrever os resultados obtidos com a execução de uma auditoria em uma empresa do mercado nacional, seguindo os procedimentos padrões utilizados pela DNV em âmbito internacional.

Dividiram-se os resultados em três situações, fatores críticos e facilitadores identificados nas etapas dos processos de execução da auditoria e os resultados da auditoria com base nos padrões adotados.

6.1 FACILITADORES

Para facilitar a análise os facilitadores foram subdivididos em duas óticas, a do cliente e da equipe auditora. Em relação ao cliente, a mais importante facilidade a ser relacionada é o fato de que é o maior conhecedor do seu Sistema de Gestão de Segurança de Informações, logo é quem domina o assunto, sabe o funcionamento, os pontos fortes e os pontos fracos.

Com relação às facilidades para a equipe auditora, foi a documentação do Sistema de Gerenciamento da Segurança de Informações já possuía uma estrutura definida nos moldes de um Sistema de Gestão da Qualidade certificado pela ISO 9001, o que em alguns aspectos são idênticos aos da BS 7799, parte 2 (manual, política, procedimentos, registros), e o pessoal envolvido com o escopo do ambiente de segurança de informações já estava ambientado com

o processo de auditoria externa, facilitando assim as entrevistas conduzidas pelo pessoal da DNV. Outro fator positivo foi o conhecimento do pessoal envolvido que já estava familiarizado com os termos e conceitos de segurança de informações que a norma determina.

Outra facilidade para a equipe é o fato da realização da visita inicial necessitar do preenchimento de um relatório. Esse relatório funciona como um *check list* para verificar se todos os documentos e processos estão sendo cobertos pelo Sistema de Gerenciamento de Segurança de Informações da organização, evitando assim que os auditores esqueçam de verificar algum documento ou atividade pertinente a essa etapa.

Como conseqüência dessa revisão de documentação, a etapa seguinte da auditoria inicial também fica facilitada em virtude de a equipe já ter obtido as informações básicas para poder localizar e questionar as pessoas e atividades que deverão ser verificadas.

6.2 FATORES CRÍTICOS

Em relação aos fatores críticos, também dividiram-se em duas óticas, a do cliente e da equipe auditora.

Em relação ao cliente foram percebidas as seguintes dificuldades:

a) o cliente tem dificuldades em identificar os seus próprios ativos (sistemas de informação) dentro da sua própria organização e negócio. Esse fato, por sua vez, pode desencadear a falta de identificação de que ativos ou sistemas de informação são os considerados críticos pela direção da empresa e, como efeito, pode ocorrer uma aplicação de análise de risco de forma equivocada, considerando ativos que não precisariam estar sendo analisados ou deixando de avaliar algum que seria essencial estar sob análise. Esse tipo de situação gera um efeito dominó, pois a partir da identificação dos ativos críticos e da análise de risco, as atividades de controle citadas na BS 7799 serão selecionadas para diminuir ou reduzir os riscos associados a esses ativos, e, se a empresa não conseguir realizar essa etapa do processo de forma satisfatória, todas as demais etapas do processo podem de alguma forma apresentar também algum tipo de problema;

b) a troca de escopo pode comprometer a abrangência dos controles;

c) o entendimento dos fatos identificados na visita inicial e a necessidade de tomar ações corretivas podem atrasar os prazos estipulados pela organização em relação à finalização do processo de certificação;

d) identificar a legislação aplicável ao negócio ou cumpri-la quando já identificada;

e) o estado de ansiedade dos colaboradores, em virtude do processo de auditoria, pode gerar dificuldades nos mesmos em demonstrar a real condição de implementação do Sistema de Gerenciamento de Segurança de Informações da organização.

Em relação à equipe auditora, as dificuldades percebidas foram:

a) identificar de forma clara, pelo menos até a visita inicial, o escopo que a empresa estará propondo e, como conseqüência disso, as atividades e os endereços que estarão sob o escopo da certificação do Sistema de Gerenciamento de Segurança de Informações. O que se percebe é que a empresa não possui a cultura de definir um escopo de atuação. Então, ao ser solicitada essa definição no questionário, para preparação da proposta, podem ocorrer dificuldades dos clientes em compreender esse questionamento e, por conseqüência, a DNV pode dimensionar uma carga de auditoria inadequada para realizar a auditoria nesse cliente;

b) outra questão associada à definição de homens-dia para a realização de trabalho é a diferença na forma de execução da etapa de pré-auditoria ou visita inicial, onde os colegas da DNV da Inglaterra utilizam parte do tempo apenas para realizar a verificação da documentação do cliente, freqüentemente antes mesmo da própria visita inicial acontecer e, no mercado nacional, a DNV procura realizar essa verificação no próprio cliente, tentando aproveitar o tempo de forma mais prática, conhecendo a documentação e solicitando explicações sobre a mesma;

c) esta forma de interpretar a instrução de processo sobre as visitas iniciais também gera uma outra diferença na realização da atividade, o auditor da Inglaterra procurou apenas a leitura da documentação, e o cliente por sua vez demonstrou

em muitas ocasiões a necessidade de participar fornecendo informações e gerando assim um certo desconforto em ambas as partes;

d) geralmente, ao finalizar a etapa da visita inicial, o cliente solicita uma previsão de tempo para execução da próxima etapa, que é a de certificação. Entretanto, esse parecer é complicado de ser emitido pela equipe auditora, uma vez que esta não tem condições de saber quais serão os recursos destinados à tomada das ações necessárias para atender aos fatos identificados;

e) a falta de familiaridade, com termos particulares de cada organização, pode dificultar o levantamento de evidências de conformidade do Sistema de Gerenciamento da Segurança de Informações, principalmente quando da realização das entrevistas com os auditados;

f) identificar, conhecer e aplicar a legislação pertinente ao negócio da organização e avaliar o impacto desta sobre o ambiente de Segurança de Informações.

6.3 RESULTADOS DA AUDITORIA

Pode-se concluir que o processo de auditoria envolve normalmente um número maior de dificuldades entre as partes envolvidas do que propriamente facilidades. Porém, apesar disso, os modelos padrões que são aplicados a esse processo permitem que a atividade de auditoria seja realizada com a obrigatoriedade de seguir alguns critérios, além dos da norma obviamente, que permitem à equipe auditora e também ao cliente buscar o entendimento e, por conseqüência, atingir os objetivos de ambas as partes.

Sendo assim, considera-se que os objetivos específicos deste trabalho foram atendidos, identificando as facilidades e dificuldades do modelo de processo de auditoria de um Sistema de Gerenciamento de Segurança de Informações baseado na Norma BS 7799, parte 2, e também avaliar os resultados da aplicação dos padrões internacionais utilizados pela DNV em outros países do mundo.

Em relação ao trabalho de pesquisa, conclui-se que o método utilizado para realização deste trabalho foi adequado, pois as etapas previstas no modelo de um processo de auditoria e os passos que podem ser utilizados para realização de um estudo de caso, são perfeitamente compatíveis e permitem que sua realização seja feita de forma concomitante, o

que facilita a execução das atividades. Porém, é importante ressaltar que para a realização adequada das etapas prevista no estudo de caso, o treinamento e experiência do entrevistador são requisitos fundamentais, pois em muitas situações é esta habilidade que permitirá ao pesquisador decidir em encerrar as averiguações ou prossegui-las.

Entretanto, algumas sugestões se fazem pertinentes para a realidade do mercado nacional, que são:

a) em relação à definição do número de homens-dia, o setor comercial deveria procurar encaminhar a solicitação de proposta de contrato para os auditores qualificados na Norma BS 7799, para que estes possam avaliar as informações contidas no formulário e contatar com o possível cliente, a fim de esclarecer eventuais dúvidas que existam, facilitando assim a definição da carga adequada de auditoria para o possível cliente;

b) em relação à execução da visita inicial, o critério de dimensionar um período para verificar somente a documentação parece mais apropriado, uma vez que essa etapa funciona como um facilitador para a compreensão do Sistema de Gerenciamento de Segurança de Informações pela equipe auditora;

c) em relação ao processo de auditoria, em virtude do assunto ser relativamente novo no mercado nacional, a etapa da visita inicial deve concentrar esforços em identificar qual é a atividade da organização e quais são os seus ativos mais importantes, uma vez que esse processo é crítico para a definição dos controles adequados e também na tentativa de reduzir ou eliminar incidentes de segurança dentro da organização.

6.4 SUGESTÃO PARA TRABALHOS FUTUROS

Sugere-se ampliar a realização da pesquisa, incluindo a avaliação da implantação da Norma BS 7799, parte 2, em organizações que tenham sido certificadas, a fim de avaliar a efetividade desse sistema.

O presente estudo procurou identificar as facilidades e dificuldades da utilização de procedimentos padrões na realização de auditoria em Sistema de Gerenciamento de Segurança de Informações com base na BS 7799, parte 2. Sugere-se também pesquisar em relação aos

clientes de uma organização certificada em BS 7799, parte 2, se existiram mudanças perceptíveis em relação ao tratamento das informações e/ou ativos por essa organização então certificada e também da viabilidade de utilizar estes modelos padrões na certificação de outras normas de gerenciamento, tais como qualidade, ambiente, saúde segurança ocupacional e responsabilidade social.

REFERÊNCIAS

AEXIS SECURITY CONSULTANTS – **BS 7799 Certification – A European Case Study**, 2001. Disponível em: http://www.aexis.de. Acessado em: 05 ago. 2001.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Sistemas de gestão da qualidade – fundamentos e vocabulário,** NBR ISO 8402:1994. Rio de Janeiro: ABNT, 1994.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Normas de gestão da qualidade e garantia da qualidade – Parte 3: Diretrizes para a aplicação da NBR ISO 9001 ao desenvolvimento, fornecimento e manutenção de software,** NBR ISO 9000-3:1997. Rio de Janeiro: ABNT, 1997.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Sistemas de garantia da qualidade – requisitos**, NBR ISO 9001:1994. Rio de Janeiro: ABNT, 1994.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Sistemas de gestão da qualidade – fundamentos e vocabulário**, NBR ISO 9000:2000. Rio de Janeiro: ABNT, 2000.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Sistemas de gestão da qualidade – requisitos,** NBR ISO 9001:2000. Rio de Janeiro: ABNT, 2000.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Sistemas de gestão da qualidade – diretrizes para melhorias de desempenho**, NBR ISO 9004:2000. Rio de Janeiro: ABNT, 2000.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão da qualidade e elementos do sistema da qualidade – Parte 1: Diretrizes**, NBR ISO 9004-1:1994. Rio de Janeiro: ABNT, 1994.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão da qualidade e elementos do sistema da qualidade – Parte 2: Diretrizes para serviços**, NBR ISO 9004-2:1994. Rio de Janeiro: ABNT, 1994.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão da qualidade e elementos do sistema da qualidade – Parte 3: Diretrizes para materiais processados,** NBR ISO 9003-2:1994. Rio de Janeiro: ABNT, 1994.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Processos de ciclo de vida de software,** NBR ISO/IEC 12207:1999. Rio de Janeiro: ABNT, 1999.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Código de prática para a gestão da segurança da informação**, NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT, 2001.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Auditorias internas de qualidade e meio ambiente,** NBR ISO 19011:2002. Rio de Janeiro: ABNT, 2002.

BEUREN, I. M. **Gerenciamento da informação: um recurso estratégico no processo de gestão empresarial.** São Paulo: Atlas, 2000.

BIO, S.R.F. **Sistemas de informação: um enfoque gerencial**. São Paulo: Atlas,1985.

BRITISH STANDARD. **Information security management – Part 2: Specification for information security management systems**, BS 7799-2:1999. London: BSI, 1999.

CARUSO, C.A.A.; STEFFEN, F.D. **Segurança em informática e de informações.** São Paulo: Senac, 1999.

DAVENPORT, T. H.; ECCLES, R.G.;PRUSAK, L. Information politics. **Sloan Management Review**, Knoxville, v.34, n.1, p.53-65, fall 1992.

DAVIS, G.B.; OLSON, M.H. **Sistemas de información gerencial.** Bogotá: McGraw-Hill, 1987.

DNV. DET NORSKE VERITAS LTDA. **Procedimentos DNV - International Certification Processes.** Disponível em: http://one.dnv.com intranet. Anexo A, acesso restrito funcionários. Acessado em: 14 jul.2002.

DNV. DET NORSKE VERITAS LTDA. **Marketing BS 7799.** Apresentação disponível em: http://one.dnv.com intranet. Acesso restrito funcionários. Acessado em: 14 jul.2002.

DNV. DET NORSKE VERITAS LTDA. **Dados da empresa.** Disponível em: http://www.dnv.com. Acessado em: 10 mar.2003.

FAGUNDES, E. M. **Cobit um kit de ferramentas para a excelência na gestão de TI**. Disponível em: http:// www.efagundes.com/artigos. Acessado em: 07.jan.2004.

FITZSIMMONS, J.A.; FITZSIMMONS, M. **Administração de serviços: operações, estratégia e tecnologia de informação.** Porto Alegre: Bookman, 2000.

FREITAS, H. M. R.; LESCA, H. Competitividade empresarial na era da informação. **Revista de Administração**, São Paulo, p. 92-102, jul/set. 1992.

FREITAS, H. M. R.; BECKER, J. L.; KLADIS, C. M.; HOPPEN, N. **Informação e decisão: sistemas de apoio e seu impacto.** Porto Alegre: Ortiz, 1997.

FURLAN, J.D. **Como elaborar e implementar o planejamento estratégico de sistemas de informação.** São Paulo: Makron, McGraw-Hill, 1991.

KENDALL, K. E.; KENDALL, J. E. **Systems analysis and design.** New Jersey: Prentice-Hall, 1999.

KINI, R.B. Strategic information systems: a misunderstood concept? **Information Systems Management**, Boston, v.10, n.4, p.42-45, fall 1993.

KUGLER, J. L. C.; FERNANDES, A. A. **Planejamento e controle de sistemas de informação**. Rio de Janeiro: LTC, 1984.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação**. Rio de Janeiro: LTC, 1999.

MENDES, C. D. Informática e competitividade da empresa. **Anais do XX Congresso Nacional de Informática**, SUCESU, São Paulo, p.175-180, 1987.

MINTZBERG, H.; QUINN, J.B. **O processo da estratégia.** Porto Alegre: Bookman, 2001.

MÓDULO S.A. **7a pesquisa sobre segurança de informação**, 2001. Disponível em: http://www.modulo.com.br. Acessado em: 1º dez. 2001.

MÓDULO S.A. **8a pesquisa sobre segurança de informação**, 2002. Disponível em: http://www.modulo.com.br. Acessado em: 5 out. 2002.

MOREIRA, N. S. **Segurança mínima: uma visão corporativa da segurança de informações**. Rio de Janeiro: Axcel Books do Brasil, 2001.

MURDICK, R.G.; MUNSON, J.C. **Sistemas de información administrativa**. México: Prentice-Hall Hispano Americana, 1988.

NASCIMENTO, L. O. S. Sistema de informações. In: MORGADO M.G.; GONÇALVES M.N. (Orgs). **Varejo, administração de empresas comerciais**. São Paulo: Senac, 1997.

OLIVEIRA, A.C.M. da C.; GRAJEW, J. O enfoque do valor adicionado: informática e aumento de competitividade. In: SUCESU, **Anais do XX Congresso Nacional de Informática**, p.190-195, 1987.

PORTER, M.E.; MILLAR, V.E. How information gives you competitive advantage, **Harvard Business Review**, Boston, v.63, n.4, p.149-160, 1985.

PORTER, M.E. **Estratégia competitiva: técnicas para análise de indústrias e da concorrência.** Rio de Janeiro: Campus, 1986.

PORTER, M.E. **Vantagem competitiva: criando e sustentando um desempenho superior**. Rio de Janeiro: Campus, 1992.

TAURION, C. Em busca de qualidade. **Computerworld**, São Paulo, p. 14-15, jun. 1996.

TOFLER, A. **A empresa flexível.** Rio de Janeiro: Record, 1985.

WATSON, R. T; KELLY, G. G.; GALLIERS, R. D.; BRANCHEAU, J. C. Key issues in information systems management: an international perspective. **Journal of management information systems.** Armonk, v.13, n.4, p. 91, 1997.

WEBER, K. C.; ROCHA, A. R. C.; NASCIMENTO, C. J. **Qualidade e produtividade em software.** São Paulo: Makron Books, 2001.

ISMS. International user group. **Registrer Certificates**, Disponível em: http:// www.xisec.com . Acessado em: 10.set. 2002.

YIN, R. K. **Estudo de caso: planejamento e métodos.** Porto Alegre: Bookman, 2001.

GLOSSÁRIO

Para subsidiar o leitor, especialmente aquele que não está familiarizado com os termos específicos da área da informática, entendeu-se como necessário conceituar e diferenciar alguns desses termos, citados a seguir.

Dados: Dados são registros de fatos ou eventos e podem ser representados por meio de imagens, sons, números, datas, etc.). Geralmente são utilizados para atividades operacionais em empresas, tais como cadastro de produtos em estoque, vendas, cadastros de clientes e atendimentos.

Informações: Informações são dados organizados e utilizados para suporte à tomada de decisões em empresas. Por exemplo, com dados, como a data de nascimento dos clientes de uma empresa, é possível gerar uma informação como a idade média dos mesmos. Demais exemplos de informação são: produtos mais vendidos, total mensal de vendas, clientes que mais compram, totais de comissões de determinado vendedor.

Sistemas de informação: São sistemas baseados em computador que transformam dados em informação. Sistema de informação são o conjunto interdependente das pessoas, das estruturas, das tecnologias da informação, dos procedimentos e métodos, que deveriam permitir à organização dispor, no tempo desejado, das informações de que ela necessita ou necessitará para o seu funcionamento atual ou para a sua evolução.

Tecnologia da Informação: Tecnologia da informação é o conjunto de software e hardware.

ANEXO A

International Certification Processes – ICP’s.

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.2-ax-ISMS QUOTATION & QUOTE REVIEW

SERVICE SPECIFIC PROCEDURE – Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.2.

See attach **Guidance** information for estimating man-days for ISMS audits.

2.2 Check on Quote Details

The following points should be considered when preparing a quote:

- Exact locations (geographically, industrial/mixed/residential area)
- Number of sites with Business activities, including any disaster recovery site, Business activities on site and number of staff at each site.
- Level of security control required for business or customer reasons; e. g. military, safety, personal privacy, commercial confidentiality
- Activities within the scope which is performed "off-site"; e. g., on customer premises, disaster recovery premises
- Major features of information technology in use - inclusive of added requirements due to specific contract, reference documents applicable to the organisation,
- Major information processing services for each type of user; e. g., personnel, finance, sales including customers and suppliers (if applicable) - inclusive of number of users in each area
- The positions or groups directly responsible for administering security management (i. e. Policy Definition, Procedure Writing, Site Security, Systems Administrator, Virus Protection, Security Incident, Data Protection)
- Security products/tools in use (Site Access; e. g., badge reader, IT System Access Control, Virus Control, Environment monitoring (computer room), Power Backup; e. g., generator, Power supply correction (UPS))
- Brief description of structure of documented information security management system; e. g., policy, security manual, work instructions
- Brief description of risk analysis method used to identify and evaluate risk.

- Statement of Applicability, or equivalent document, which identifies the controls of BS 7799 which are applied.
- Copy of any ISO 9001/2 (or ISO 9001:2000) certificate applicable to the organisation

Checklist of attachments to the application:

1. Security system contents pages
2. Risk analysis report
3. Statement of Applicability
4. ISO 9000 certificate or other certificates

2.4 Time and Price Estimation of Audit/Pre-assessment

Pricing of BS 7799 certification may be the same day rates and other features of the pricing structure as for ISO 9000 certifications, use the **Guidance** information to estimating man-days found in this appendix. The new table will account for the fact that BS 7799 is normally a more complex audit with more complex businesses.

These rates may be adjusted by the units (and then the ICP) as experience is gained performing this service.

While ISMS certificates must be independent of those for ISO 9000, an applicant who has ISO9000 certification already or, who is applying for both, may be quoted for combined audits. There is a degree of overlap between the two (e.g. in respect of policy, documentation of procedures, maintenance of records, conduct of audits) such that some time may be saved by combining visits. As a rule of thumb, timesaving should not exceed one workday on the larger audits (over 6 workdays) or a half workday between 3 and 6). Below 3 workdays there will be no effective saving.

2.4.1 Periodic Audits

The rules regarding the frequency of periodic audits are the same as for ISO 9000 (see ICP C5-ce-3.13 "Periodic Audits"). The special requirements of the TickIT scheme do not apply so annual periodic visits can be offered on the usual basis.

2.4.7 Multiple Site Certification and/or Verification

Multiple sampling decisions in the area of ISMS certification are more complex than the same decisions are for quality systems. Certification bodies wishing to use a sample based approach to multiple site assessment need to maintain procedures which include the full range of issues below in the building of their sampling programme.

Prior to undertaking its first assessment based on sampling, the certification/registration body shall provide to the accreditation body the methodology and procedures which it employs and provide demonstrable evidence of how these take account of the issues below to manage multiple site ISMS assessment.

The certification body's procedures should ensure that the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where an organisation has a number of similar sites covered by a single ISMS, a certificate may be issued to the organisation to cover all such sites provided that:

1. All sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review

2. All sites have been audited in accordance with the organisation's internal security review procedure(s)

3. A representative number of sites have been sampled by the certification body, taking into account the requirements below:

- The results of internal audits of head office and the sites
- The results of management review
- Variations in the size of the sites
- Variations in the business purpose of the sites
- Complexity of the ISMS
- Complexity of the information systems at the different sites
- Variations in working practices
- Variations in activities undertaken
- Potential interaction with critical information systems or information systems processing sensitive information
- Differing legal requirements

1. The sample should be partly selective, based on the above in point c, and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection.

2. Every site included in the ISMS which is subject to significant threats to assets, vulnerabilities or impacts should be audited by the certification body prior to certification.

3. The surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the organisation or within the scope of the ISMS certification included in the Statement of Applicability

1. In the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites covered by the certificate.

2.4.9 Shared Site

Special considerations should be given to shared sites; i. e. where several companies share the same facilities. It is permissible to carry out certification for a business which is part of a shared site, subject to the following conditions:

- The organisation must have been clearly identified and be managing its interfaces with other businesses/organisations on the site
- The organisation must have identified all significant aspects, in connection with the other activities on the site, and must be influencing or seeking to influence them by either formal objectives (improvement or investigation) or operational control.

2.4.10 Service Organisations

Where it is not practical to define a location, the coverage of the certification shall take into account the customer's headquarters activities as well as delivery of its services.

Where relevant, in special cases, the certification may be carried out only where the customer delivers its services. In such cases, the interfaces with its headquarters shall be audited.

Guidance on man-day allocation for BS 7799 assessments
DRAFT version 1 – February 2001

The following guidance may be used to estimate the man-days needed to perform a BS-7799 audit. This draft table has been submitted to the European Co-operation for Accreditation for comments/acceptance by SWEDAC.

1.1 Definitions

Company Structure: scope/boundaries, group (of companies), co-operation partners, geographical spread (not the IT-part)

Size: number of employees (Small ≤ 50; 50 ≤ Medium ≤ 250; Large ≥ 250)

IT-structure: configuration complexity, platform(s), dependence on IT, external connections, etc.

Risk level: business activity (impact on society, vulnerability, secrecy…), critical competence (dependant on competence in the business activity)

COMPLEXITY EVALUATION

Estimation of time level

CATEGORY				IMPACTING FACTORS (BUSINESS ACTIVITY/COMPANY STRUCTURE)
H				Medium to large size group/company/unit with business activities including most functions, i.e. R&D, design/development, production and/or construction, service. Business at several locations. A number of co-operations partner. Eventually business activities in several countries. Special legal requirements.
	M			Medium to small size company/unit with 1-2 business areas including R&D, design/development, production and/or construction, service.
		L		Medium to large company with production and/or construction with limited activities within design/development. A single country, a limited number of co-operation partners, eventually some specific legal requirements.
				Small to medium company/unit with production and/or construction with limited activities within design/development.
				Small to medium company/unit with installation/service/sales. Mainly business on one location, single or few co-operations partners - no special legal requirements.

CATEGORY				IT-STRUCTURE
H				Several externally connected Extra-Nets. A number of non-standard real-time applications on several platforms. Potential interaction with critical information systems or information systems processing sensitive information.
	M			External fixed connection from a home work place. Sharing of facilities (e. g. computers, telecommunication systems, etc.) with others. Complexity of information systems. Development of own software applications used in the organisation.
		L		A single or several connected LANs. Fixed connection to the Internet (ISDN, Broadband, etc.) and information WEB-site for clients. Only standard applications on one platform.
				Single local area network with some workstations and or personal computers. E-mail handling via the Internet via a dialled-up modem connection.
				No network – a standalone personal computer or a single local area network with some workstations. No external connections.

Estimation of impacting factors / IT-structure for ISMS Certification

IMPACTING FACTORS/ IT-STRUCTURE	LOW (man-days)	MEDIUM (man-days)	HIGH (man-days)
LOW	3-4	5-7	7-10
MEDIUM	4-5	6-10	8-14
HIGH	5-6	7-12	9-18

Estimation of Man-days for ISMS Certification (One of the below)

The table below shows the distribution of the above estimated man-days for the certification activity.

IMPACTING FACTORS/ IT-STRUCTURE	Pre-Assessment	CERTIFICATION				Maintenance of Certificate (per year)
		Documentation Review	Initial Audit, step 1	Initial Audit, step 2	Estimated TOTAL for certification	
Low - Low	1-4	1	1	1-2	3-4	1-2
Low-Medium	1-7	1-2	2	2-3	5-7	2-4
Low - High	2-10	2	2-3	3-5	7-10	3-6
Medium - Low	1-5	1	1-2	2	4-5	2-4
Medium - Medium	1-10	1-2	2-3	3-5	6-10	3-6
Medium - High	2-14	2	2-3	4-9	8-14	4-8
High-Low	1-6	1	2	2-3	5-6	2-4
High - Medium	1-12	1-2	2-3	4-7	7-12	3-7
High - High	2-18	2-3	3-4	4-11	9-18	4-10

Note: Initial Audit – step 1 consist of the Initial Visit + the part of the Initial Audit (technical system review)

Special considerations must always be taken into account on the need of a technical expert during audits. The need of an extra technical expert is based on the IT-complexity of the organisation and the knowledge of the auditor.

Should there be a large amount of multiple sites the number of auditing man-days needs to reflect this.

Please refer to "EA-7/03 – EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems" for further aspects to consider during estimations on efforts.

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.7-ax-ISMS DOCUMENT REVIEW

SERVICE SPECIFIC PROCEDUR - Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3-7.

2.1 Review Documentation

The documentation to be reviewed shall consist of, as a minimum:

- Policy Statement/Document
- Risk Analysis Documentation
- Statement of Applicability
- Scope of ISMS document
- Organisational structure
- Description of the technology including a network schematic
- Security Policy Manual that should include the following (much the same as given above, but in one manual):
- Security policy, both full and the short version
- The nature of the organization and its corresponding security needs
- Security management framework – how the organization manages security
- Description of the information security management system (ISMS)
- Procedures for the operation and maintenance of the ISMS
- Documentation and records structure with references to the lower level documents
- Security scope, defining the limits of the security management framework
- Description of the risk assessment system
- A summary of the implemented controls and safeguards

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.8-ax-ISMS INITIAL VISIT

SERVICE SPECIFIC PROCEDURE – Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.8.

2.1 Initial Visit preparation

For the initial visit preparation, the following is required:

- An evaluation of the risk analysis, as specified in the risk analysis report, should be completed - taking into account the specified security products/tools in use.
- A review of the statement of applicability should have taken place.
- A review of the level of security control required, as specified by the organisation.
- A review of the major features of the information technologies in use - including a network plan.
- A review of the information processing services for each type of user.
- An agreement of the nature of confidentiality in place; that is, there should be no doubt as to the access for the auditor(s) to personnel records, etc. within the organisation.

2.2 Conduct of the Initial Visit

Access to personnel records

The lead auditor should verify that auditors will be given access to all relevant records needed for effective assessment of the ISMS.

Risk Analysis / Assessment

The lead auditor/verifier shall discuss the customer's risk analysis/assessment and the means by which they have evaluated significance. The aim of this is to establish that the organisation's risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS standard or normative document.

Statement of Applicability

The lead auditor/verifier shall discuss the customer's statement of applicability. The aim of this is to establish correct understanding of defines terms as well as that the statement of applicability correctly reflects the organisations information security scope.

Reliance on Internal Audits

The lead auditor/verifier shall establish whether the internal audit frequency is related to information security aspects.

The team leader shall make the customer aware that the following additional information may be required for detailed inspection during the initial audit:

- Personnel records of confidential nature.
- Details of any internally identified non-conformities together with details of relevant corrective and preventive action taken in the previous 12 months (or since commencement of system implementation if this is less than 12 months)
- Records of management reviews
- Records of any system related communications received and any actions taken in response to them.

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.10-ax-ISMS ASSESSMENT PROCESS: INITIAL AUDIT

SERVICE SPECIFIC PROCEDURE – Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.10.

1.1 Objectives

An additional objective for these types of audit is to:

- Determine that the organisation has not excluded from the scope of their ISMS elements of their operation which should properly be included under it.
- Ensure that the organisation's risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS standard or normative document.
- Confirm that the organisation's risk assessment is reflected in the organisation's statement of applicability.
- Ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the risk assessment.
- Determine whether the established, implemented and documented ISMS system is working to ensure legal compliance
- Determine whether the ISMS is meeting of the companies' objectives & target with respect to IS, and
- Determine whether the implemented ISMS properly protect information and computer assets.

The audit should focus on the customer's compliance to the information security requirements (elements) as given below:

- Management Framework (Policy, SoA, etc.)
- Implementation
- Documentation
- Document Control
- Information Security Control Measures to include:
- Security Policy
- Security Organisation
- Assets Classification and Control
- Personnel Security
- Physical and Environmental Security
- Computer and Network Management
- Systems Access Control

- Systems Access Control
- System Development and Maintenance
- Business Continuity Planning
- Compliance

1.1 Audit Opening Meeting

The lead auditor should verify that auditors will be given access to all relevant records needed for effective assessment of the ISMS.

1.2 Conduct of the Audit

The integration of the ISMS audit with Q, E, or S would:

- Have the same common elements as in item 2.3 a) in document ICP C5-ce-3.10 and there could be assessed by any of the lead auditors.
- As for item 2.3 b) same reference, the ISMS lead auditor would have to assessment his respect part.

Critical areas such as the information security control measures (see 2.1 above) shall be audited by the ISMS lead auditor (with possible assistance from an ISMS qualified auditor or specialist).

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.13-ax-ISMS PERIODIC AUDIT

SERVICE SPECIFIC PROCEDURE – Safety Contractor Checklist (SCC)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.13.

2.1 Periodic Audit Plan

Periodic audits must be scheduled and performed in accordance with ISO 10011. The periodic audit plan, drawn up at the conclusion of the initial visit, shall demonstrate that all relevant requirements will be reviewed during the three-year cycle.

2.3 Periodic Audit

Controls which must be reviewed on every visit include:

- audits of operational systems
- handling of complaints
- handling of security incidents
- conduct of security reviews
- correct use of certificate and logos

Additional visits may be required following significant changes to the certified organisation or its security management approach, or in case of failure to implement satisfactory correction of non-conformities.

Accredited BS 7799 certification requires three yearly re-certification audits. The re-certification audit shall be planned at the prior periodic audit. The plan content will cover the same issues as for the initial certification, including reconfirmation that the customers' products, services and markets are still consistent with the Statement of Applicability (SoA) and hence the Information Security Management System.

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.15-ax-ISMS NON-CONFORMITIES & FOLLOW-UP OF CORRECTIVE ACTIONS

SERVICE SPECIFIC PROCEDURE – Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.15.

2.1 Classification of Non-conformities

Non-conformities would include all those identified in the Generic Process Instructions and would further include:

- No documented evidence of a performed Risk Analysis
- Missing or inadequate Business Continuity Plan
- Ambiguity, lack of clarity, lack of balance, inaccuracies, dubious factual information or misrepresentation in the Statement of Applicability
- Discrepancies between the information in the Statement of Applicability and verification of the information on site.

DNV MANAGEMENT MANUAL PROCEDURE
INTERNATIONAL CERTIFICATION PROCESSES

C5-ce-3.16-ax-ISMS DEFINITION OF SCOPE & STANDARD

SERVICE SPECIFIC PROCEDURE – Information Security (BS 7799)

The section numbering below follows what is found in section 2 of ICP C5-ce-3.16.

2.1 Guidance on scope

Organisations should define the scope of their ISMS. A role of the certification body is to provide consistency in ensuring that organisations do not exclude from the scope of their ISMS elements of their operation which should properly be included under it.

Certification bodies should ensure that the organisation's risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS standard or normative document. Certification bodies should confirm that this is reflected in the organisation's statement of applicability.Interfaces with services or activities that are not completely within the scope of the ISMS should be addressed within the ISMS subject to certification (e. g. they should be included in the risk assessment).In addition to the detailed site description, the scope shall definitely define which site or sites or parts of the site(s) are covered by the certificate.

The activities of the customer should be identified in terms of general descriptions of the main activities.

It should be clear where the boundaries of management responsibility extend, for example in respect of a company that shares a site with another company.

It shall also be made clear if any major activities are excluded, for example warehousing or sales & marketing, etc.

In summary, the scope of the certification audit should state:

- Site(s) identification
- Main activities
- Exclusions

ANEXO B

Quotation Request

DET NORSKE VERITAS Certification

MANAGEMENT SYSTEM CERTIFICATION

QUOTATION REQUEST

In order to allow us to provide as accurate a quote as possible, we need to determine exactly what sort of process and activities are involved within your organisation. We also need to know about the state of readiness of your Management System prior to certification.

Please provide us with as much detail as you can by answering the following questions. If you have any queries, please contact us on:

☎ 020 7357 6080 Fax: 020 7407 1239E-mail: certificationuk@dnv.com

Section 1: Basic Contact Information

1.1 Company or Organisation Name	
1.2 Contact Name	
1.3 Position	
1.4 Address	
1.5 Telephone Number	
1.6 Fax Number	
1.7 E-mail Address	
1.8 Website Address	

Section 2: Organisational Details

2.1 Please describe fully the products, process and/or services of your organisation.

Note. Append any useful further information to the application form. For example, company promotional literature, or your Quality Management System (ISO 9000) scope.

2.2 Is your organisation part of a larger group?	**NO**		**YES**	

If no, please go to question 2.4.

2.3 Name of Parent or Holding Company:	

2.4 Total Number of Employees to be covered by certificate:	

Comprising of:

2.41 Managerial		**2.43 Production**	
2.42 Technical		**2.44 Administration**	

2.5 Do any staff work shifts?	**NO**		**YES**	

If no, please go on to question 2.7

2.6 Number of Staff Working Shifts:	

Shift Details:

2.7 Are other sites to be covered ?	**NO**		**YES**	

If no, please go on to question 2.9

2.8 Please describe fully the locations, staffing, products, process and/or services of the other sites within the scope of your management system

Note: Continue on separate sheets as required.

2.9 Does the system cover other offsite activities?	NO		YES	

Note: This would include temporary sites, such as construction locations, major projects, installation, servicing and maintenance operations, disaster recovery sites. If no, please go on to Section 3.

2.10 Please describe fully these activities, giving locations and duration of projects and personnel numbers

Section 3: Your Requirements

3.1 Please indicate the management system standard(s) required, and please complete additional information as indicated:		
	1.1	
ISO 9001: 2000 (New client)		Please Complete Section 4 (click here)
ISO 9001: 2000 (Transfer for existing client)		
ISO 9001: 1994		
ISO 9002: 1994		
TickIT		
QS 9000		
ISO 14001		Please complete Section 5 (click here)
EMAS		
OHSAS 18001		Please complete Section 6 (click here)
BS 7799		Please complete Section 7 (click here)
VCA/SCC		

Note: Accredited certification against ISO 9001:2000 will be available following the implementation of the standard.

3.2 Do you require a pre assessment?				
	NO		**YES**	

Note: The pre assessment is an optional “gap analysis” typically of one or two days in duration. It is very valuable in identifying to you at an early stage potential areas of concern at the subsequent certification audit. If no, go to question 3.4

3.3 Do you require a written report?				
	NO		**YES**	

Note: This is typically an extra day of off-site reporting.

3.4 Are any parts of your management systems already certified/registered ?				
	NO		**YES**	

If no, go to question 3.6

3.5 Please indicate the standard(s) and the certification body.

Note: You may be registered with another certification body. We can assure you that dealing with more than one certification body will not complicate your situation.

3.6 Are you interested in a quotation including conversion of your existing certification to DNV?				
	NO		**YES**	

3.7 Please indicate your preferred date of commencement of assessment:

3.8 Please indicate whether further information has been enclosed with your application.				
	NO		**YES**	

Finally, please sign and date the quote request form below:

Name:		**Position:**	
Signature		**Date:**	

The information supplied above will be used to provide you with a quotation for our certification services. This quotation is totally dependent upon the information given above. We must therefore reserve the right to amend our quote should the information be found to be inaccurate or incomplete.

Please post, fax or e-mail the completed form to us at:

DNV Certification Ltd
Palace House
3 Cathedral Street
London
SE1 9DE
Fax: **020 7407 1239**
E-mail: **certificationuk@dnv.com**

Section 4: Quality Profile

Please append any publicly available information relating to your organisation and quality management system.

New Certification Clients:

Note: existing ISO 9000 clients seeking transfer to ISO 9001:2000 go to question 4.2

4.1 Management system development:		
	YES	**NO**
Do you have a quality policy?		
Have you prepared a process orientated, documented system description?		
Have all staff been made aware of the management system?		
Has an internal audit programme started?		
Has a management review been carried out?		
Are there any requirements of ISO 9001:2000 that should be excluded from the certificate scope (e.g. design)? If yes please indicate below.		
Scope Exclusions:		

Existing Certification Clients Seeking Transfer to ISO 9001:2000

Note: please complete these questions based on projected date for transfer audit taking place.

4.2 Transfer of existing clients to new ISO 9001:2000 Standard:		
Please indicate when you would like the transfer audit to take place (Note 1)		
	YES	**NO**
Do you want a transfer audit resulting in issue of a new 3 year certificate? (Note 2)		
Has the existing QMS been reviewed and modified to meet ISO 9001:2000?		
Has the modified system been in place for sufficient time for you to evaluate effectiveness and compliance with ISO 9001:2000?		
Are there any requirements of ISO 9001:2000 that should be excluded from the certificate scope (e.g. design)? If yes please indicate below.		
Scope Exclusions:		

Note 1: our recommended approach is to undergo the transfer/upgrade audit at your scheduled certificate renewal (reassessment) audit, or at a scheduled periodic audit.

Note 2: our standard quotation will be for a full transfer/upgrade to ISO 9001:2000 resulting in issue of a new 3-year certificate.

4.2 Are you interested in services associated with ISO 9001:2000 gap analysis and auditing?	**NO**		**YES**	

Return to Main Form

Section 5: Environmental Profile

Please append any publicly available information relating to your organisation and environmental management.

5.1 Please describe your organisation's site, its geographical location and type of environment.

Note: Please indicate if there are sites of high nature conservation interest in close proximity to the site

5.2 Do you operate an IPPC, IPC or Local Authority prescribed process (UK only)?	**NO**		**YES**	

5.3 Please provide details on all key regulations, including authorisations, consents and licences relating to your sites and operations.

5.4 Does the organisation subscribe to any environmental Codes of Practice?	**NO**		**YES**	

If no, please go on to 5.6.

5.5 Please list key requirements below:

Note: This would include such measures as the Chemical Industries "Responsible Care" Programme, and the International Chamber of Commerce's Charter on Sustainable Development.

5.6 Technical issues:		
	YES	NO
Do you generate Special (Hazardous)Waste?		
Do you hold a consent/licence for discharge to sewer/watercourse?		
Are you a registered waste carrier?		
Is your site covered by legal requirements for hazardous installations?		
Do you own/operate on any contaminated land?		
Do you have any power generation on site?		
Do you carry out any effluent treatment on site?		

5.7 Management system development:		
	YES	NO
Has a preparatory environmental review been carried out?		
Do you have an environmental policy?		
Have you identified the significant environmental aspects?		
Have you identified applicable environmental legislation?		
Have you set environmental objectives and targets?		
Has a programme been put in place to achieve the objectives?		
Have you prepared a documented system description?		
Have all staff been made aware of the management system?		
Has an internal audit programme started?		
Has a management review been carried out?		
Has an Environmental Statement been drafted (EMAS only)?		

Return to Main Form

Section 6: Safety Profile

Please append any publicly available information relating to your organisation and safety management.

6.1 Please describe your organisations' site, its geographical location and type of environment.

Note: Please indicate if there are safety critical locations nearby.

6.2 Do you operate a process under CIMAH/COMAH requirements (UK only)?	**NO**		**YES**	

6.3 Please provide details on all key regulations, including authorisations, consents and licences relating to your site safety issues.

6.4 Does the organisation subscribe to any safety Codes of Practice?	**NO**		**YES**	

If no, please go on to Section 3.

6.5 Please list key requirements below:

Note: This would include such measures as the Chemical Industries "Responsible Care" Programme, International Safety Rating System (ISRS) etc.

6.6 Management system development:		
	YES	NO
Has a safety management review been carried out?		
Do you have an occupational health and safety policy?		
Have you identified occupational health and safety risks?		
Have you identified applicable safety legislation?		
Have you set health and safety objectives and targets?		
Has a programme been put in place to achieve the objectives?		
Have you prepared a documented system description?		
Have all staff been made aware of the management system?		
Has an internal audit programme started?		
Has a management review been carried out?		
Are emergency plans and procedures in place?		

Return to Main Form

Section 7: Information Security Management Profile

Please append any publicly available information relating to your organisation and information security management.

7.1 Brief description of the level of security control you require for business or customer reasons (e.g. military, personal privacy, commercial confidentiality):

7.2 Major features of information technology in use:	
Central processing	
Desktop equipment	
Remote/mobile equipment	
Network features	
Access by other parties	
Other key features	

7.3 Major information processing services for each type of user (e.g. personnel, finance, sales etc):		
User Group/Department	**No. of Users**	**Information Processing Services**

7.4 Management system development:		
	YES	**NO**
Do you have an ISMS policy?		
Do you have a Statement of Applicability (give reference)?		
Have you identified applicable ISMS legislation?		
Have you prepared a documented system description?		
Have all staff been made aware of the ISMS management system?		
Has an internal audit programme started?		
Has a management review been carried out?		
Please provide brief description of risk analysis method used to identify and evaluate risks:		

Return to Main Form

For Office Use Only:

NACE Classification	

Accredited Scope?	

Auditors Available:	

Audit Dates	

Result

Quote		**Decline**		**Apply for extension**	

Day Rate

Audit		**Travel**	

Initial Estimate (Mandays)

Pre Assessment	
Document Review	
Initial Visit	
Initial Audit	
Additional (e.g. EMAS finalisation)	

Periodics

Total Mandays per year	
Annual or six monthly regime	

Comments

Completed by:	
Date:	