UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

GUILHERME GONÇALVES LESSA

Gestão de Segurança da Informação: Implementação da Norma BS7799-2:2002 em uma Instituição Financeira

Porto Alegre

2006

GUILHERME GONÇALVES LESSA

Gestão de Segurança da Informação: Implementação da Norma BS7799-2:2002 em uma Instituição Financeira

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Mestre em Administração.

Orientadora: Profa. Dra. Ângela Freitag Brodbeck

Porto Alegre

2006

Lessa, Guilherme Gonçalves
Gestão de Segurança da Informação: Implementação da Norma BS7799-2:2002 em uma Instituição Financeira
109 f. : il.

Dissertação. (Mestrado) – Universidade Federal do Rio Grande do Sul, Escola de Administração, Programa de Pós-Graduação em Administração, 2006.

Orientadora: Profa. Dra. Ângela Freitag Brodbeck

1. Segurança da Informação. 2. BS7799. 3. Gestão de Risco. 4. Tecnologia da Informação. I. Título

CDU

Dedico este trabalho à Sinara.

AGRADECIMENTOS

Agradeço primeiramente a minha esposa, Sinara Pires, pelo amor, dedicação e companheirismo, sem os quais o presente trabalho não teria sido realizado.

A minha família, em especial, a meu pai, Luiz Carlos Barbosa Lessa, e a minha mãe, Nilza Gonçalves Lessa, por terem me dado as bases para que eu chegasse onde estou.

Ao Banco Matone, especialmente os Srs. Alberto Matone e Ernandi Ávila, que financiou e me possibilitou realizar o Mestrado, etapa importante de minha formação profissional, e que também me permitiu realizar esta pesquisa em suas dependências.

Aos meus colegas de trabalho, em especial a Secretária Executiva Sibele, por sua generosidade e paciência.

À Universidade Federal do Rio Grande do Sul, por me acolher e colocar toda a sua infra-estrutura à disposição de minha formação.

Aos doutores, mestres, professores e funcionários, que muito contribuíram, com sua experiência e comprometimento, para esta conquista.

À minha orientadora, Profa. Dra. Ângela Brodbeck, por seu comprometimento e competência.

Aos colegas do curso de Mestrado e aos amigos verdadeiros.

E finalmente, a um grande número de pessoas que contribuíram, direta ou indiretamente, para a conclusão desta etapa.

De coração, obrigado a todos.

RESUMO

Na sociedade contemporânea, não há dúvidas sobre a importância, a relevância e o poder que a informação possui. Nas organizações, também são crescentes a sua importância estratégica e os riscos que lhe são associados, bem como a necessidade de uma boa Gestão da Informação. Certos eventos de maiores conseqüências, tais como os ocorridos em 11 de setembro de 2001, nos Estados Unidos da América, apresentaram uma nova realidade relacionada às necessidades de um sistema para a preservação adequada de informações e aos impactos da integridade destas informações sobre a continuidade dos negócios. A partir de preocupações relacionadas a este tema, foram estabelecidos os fundamentos da Segurança da Informação. A presente pesquisa identifica quais as melhores práticas atualmente existentes para uma gestão adequada da Segurança da Informação nas organizações, a partir de um estudo de caso sobre o processo de implementação de um Sistema de Gestão de Segurança de Informação em uma Instituição Financeira de pequeno porte, baseado na norma BS7799-2:2002. Ao final do presente trabalho, será apresentado o modelo genérico resultante desta pesquisa, contendo as etapas e as atividades necessárias para a implementação de um Sistema de Gestão de Segurança de Informação, os principais componentes a serem implementados e alguns dos principais fatores críticos de sucesso desta implementação.

Palavras-chave: Segurança da Informação, BS7799, Gestão de Risco,Tecnologia da Informação.

ABSTRACT

In modern society, there is no doubt upon the importance, the relevance or the power that information possesses. Within organizations, its strategic importance and its associated risks are also growing, as well as the needs for a good Information Managing. Certain events with more significant consequences, such as the ones occurred in September 11, 2001, in the United States of America, have presented a new reality related to the necessity of an adequate system to preserve information, as well as related to this integrity impacts on business continuity. From questions concerning this subject, were established the main points of Information Security. The present research identifies the best current existing practices for an adequate Information Security Management in organizations, from a case study performed on the implementation process of a System of Information Security Management in a small size Financial Institution, based on the norm BS7799-2:2002. At the end of the present work, it will be presented the generic model that resulted from this research, containing the different steps and activities which are necessary for implementing of a System of Information Security Management, and the main components to be implemented, and some of the most critical success factors on this implementation.

Key-words: Information Security, BS7799, Risk Management, Information Technology.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

BC – Banco Central do Brasil

BS – British Standard

BSI – British Standard Institute

CCSC – Commercial Computer Security Center

CDB – Certificado de Depósito Bancário

CIFI – Certified Information Forensics Investigator

CISM – Certified Information Security Manager

CISSP – Certified Information Systems Security Professionals

CMN – Conselho Monetário Nacional

COBIT – Control Objectives for Information and related Tecnology

CVM – Comissão de Valores Mobiliários

DNV – Det Norske Veritas

DoD – Departament of Defense

DQS GMBH – Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

DTI – Departament of Trade and Industry

IEC – International Electro-Technical Commission

IFs – Instituições Financeiras

ISACA – Information Systems Audit and Control Association

ISMS – Information Security Management System

ISO – International Organization for Standardization

ITIL – Information Tecnology Infrastructure Library

MSI – Managing Security of Information

NIST – National Institute of Standards and Technology

NSA – National Security Agency

OGC – Office of Government Commerce

OSI – Open Systems Interconnection

PDA – Personal Digital Assistent

PDCA – Plan-Do-Check-Act

SGSI – Sistema de Gestão em Segurança da Informação

SLA – Service Level Agreement

SLM – Service Level Management

SOX – Lei Sarbanes-Oxley

SPB – Sistema de Pagamentos Brasileiro

STR – Sistema de Transferência de Reservas

TI – Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão destacados a importância, a relevância e o valor da informação, sua importância estratégica nas organizações atuais e os riscos associados a ela. Também serão apresentados a situação-problema, o objeto da pesquisa realizada e seus objetivos geral e específicos.

1.1 AMBIENTE ATUAL DE NEGÓCIOS

A humanidade empiricamente sempre percebeu que "conhecimento"[1] é "poder"[2] (BACON, 1627). No século XX, a partir de um número exponencialmente crescente de invenções, também mudaram a velocidade e os meios de geração, armazenamento e distribuição de conhecimento. Neste contexto, o conhecimento também pode ser chamado de "informação", e como tal possui "valor"[3]. Sob este ponto de vista, a informação está exposta a ameaças, vulnerabilidades, ataques, riscos, perdas e manipulações. A partir desta preocupação, foram elaborados os conceitos de Segurança da Informação, com o objetivo de minimizar os fatores supracitados.

Os eventos de 11 de setembro de 2001, nos Estados Unidos, estabeleceram, em todas as organizações do mundo, um "divisor de águas" quanto à preocupação com a Segurança da Informação. Ao destruir os edifícios do *World Trade Center*, os agressores literalmente pulverizaram diversas empresas que tinham na informação o

---

[1] Conhecimento: (a) procedimento compreensivo por meio do qual o pensamento captura representativamente um objeto qualquer, utilizando recursos investigativos dessemelhantes; intuição, contemplação, classificação, mensuração, analogia, experimentação, observação empírica etc.; que, variáveis historicamente, dependem dos paradigmas filosóficos e científicos que em cada caso lhes deram origem; e (b) somatório do que se sabe; o conjunto das informações e princípios armazenados pela humanidade (HOUAISS; VILLAR, 2001).

[2] Poder: supremacia em dirigir e governar as ações de outrem pela imposição da obediência, dominação, domínio (HOUAISS; VILLAR, 2001).

[3] Valor: medida variável de importância que se atribui a um objeto ou serviço necessário aos desígnios humanos e que, embora condicione o seu preço monetário, freqüentemente não lhe é idêntico ou ainda a capacidade de satisfazer necessidades; utilidade, préstimo, serventia (HOUAISS; VILLAR, 2001).

seu principal patrimônio. O ataque foi devastador. No entanto, o impacto foi diferente entre as empresas envolvidas. Enquanto algumas delas desapareceram por completo, ou faliram imediatamente após o atentado, devido à destruição total de suas informações, outras como, por exemplo, o *Deutsche Bank* (que possuía dois escritórios nas torres) já operava seus sistemas normalmente, no dia seguinte ao atentado. Isto foi possível porque este banco já havia implantado um Sistema de Gestão da Segurança da Informação e, entre as suas práticas, implantado um consistente plano de continuidade de negócios e um *site backup* com todos os dados necessários à operação em New Jersey, a poucos quilômetros do local do atentado (FARIAS JR., 2002).

Por outro lado, também nos Estados Unidos, ocorreram escândalos contábeis envolvendo grandes empresas como *Worldcom, Tyco, Enron* e *Arthur Andersen*, na manipulação de resultados financeiros, desvio de informações, fraudes contábeis e outras práticas ilícitas. Depois de apuradas as causas, iniciou-se um movimento para a regulação das empresas, que culminou com a legislação que vem transformando, de maneira significativa, as relações comerciais em todo o mundo: *The U.S. Public Company Accounting Reform and Investor Protection Act of 2002* conhecida como Lei Sarbanes-Oxley ou simplesmente “SOX”. A SOX é o ápice do regramento da boa governança corporativa, imputando obrigações e penas pesadas às empresas e seus dirigentes, em caso de desacordo entre registros e relatórios financeiros. (PEIXOTO, 2004).

No contexto das ameaças à segurança da informação, cabe salientar alguns aspectos relevantes: a importância estratégica da informação; o uso crescente, pela sociedade, de artefatos baseados na tecnologia digital; a importância da gestão estratégica da informação nas organizações; a importância da tecnologia da informação como meio e infra-estrutura para os negócios; e, finalmente, a necessidade de uma preocupação constante com a segurança da informação.

1.2 SITUAÇÃO-PROBLEMA

Uma vez identificadas a importância, a relevância e a abrangência da segurança da informação no atual contexto das organizações, em nível mundial, cabe estabelecer suas implicações no âmbito brasileiro, em especial, as relativas às Instituições Financeiras (IFs). A preocupação com a regulamentação do mercado

financeiro sempre foi uma constante, haja vista a implementação, com sucesso, em 2002, do Sistema de Pagamentos Brasileiro (SPB).

> A entrada em funcionamento do Sistema de Transferência de Reservas – STR, em 22 de abril de 2002, marca o início de uma nova fase do Sistema de Pagamentos Brasileiro – SPB. Com este sistema, operado pelo Banco Central do Brasil, o País ingressa no grupo de países em que transferências de fundos interbancárias podem ser liquidadas em tempo real, em caráter irrevogável e incondicional. Este fato, por si só, possibilita redução dos riscos de liquidação (riscos de crédito e de liquidez) nas operações interbancárias, com conseqüente redução também do risco sistêmico, isto é, o risco de que a quebra de um banco provoque a quebra em cadeia de outros bancos, no chamado “efeito dominó" (BRASIL, 2002).

O esforço realizado para o estabelecimento das bases legais para a implementação deste e de outros importantes mecanismos relacionados têm por objetivo garantir maior transparência, eficiência e segurança aos mercados, aos agentes envolvidos e, em ultima análise, à sociedade. Dentre as principais iniciativas relacionadas à segurança da informação, nesta área, podem ser observados: a Resolução 2.554/1998 do Banco Central, que dispõe sobre a implantação e implementação de controles internos (Anexo A); a Instrução CVM n° 358, de 3 de janeiro de 2002, da Comissão de Valores Mobiliários, que dispõe, entre outros tópicos, sobre a divulgação e uso de informações sobre ato ou fato relevante (Anexo B); e o Decreto n° 4.553, de 27 de dezembro de 2002, da Presidência da República, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (Anexo C).

As IFs viram-se obrigadas a dar respostas adequadas para inúmeras questões, a saber:

a) como atender aos requisitos definidos nas disposições legais (tributária, ambiental, fiscal, etc.)?;

b) como atender aos requisitos definidos nas disposições dos órgãos reguladores, tais como Banco Central ou CVM (lei das S/A, Basiléia II, SOX, etc.)?;

c) como garantir acurácia e prazos compatíveis para atendimento de informações ao Banco Central, Receita Federal, órgãos da Justiça e demais agentes públicos?;

d) como garantir a disponibilidade, continuidade dos negócios e recuperação em caso de desastre?;

e) como internalizar estes conceitos (esta nova ética) na IF e garantir o comprometimento de todos os colaboradores?;
f) como utilizar as novas tecnologias a favor dos negócios e minimizar as ameaças decorrentes de sua adoção?;
g) como atender às demandas crescentes do mercado em relação à segurança de suas operações?;
h) como garantir aos acionistas e executivos a transparência e confiabilidade das informações levadas a público?;
i) como garantir adequado alinhamento estratégico e boas práticas de Governança Corporativa?

Diante deste contexto, surgiram algumas questões de pesquisa:
a) de que forma a segurança da informação pode ser melhorada em uma Instituição Financeira (IF) de pequeno porte?;
b) como implementar um sistema de Gestão em Segurança da Informação (SGSI) em uma Instituição Financeira de pequeno porte?;
c) quais são os fatores críticos de sucesso da implementação de um sistema de Gestão de Segurança da Informação em uma Instituição Financeira de pequeno porte?

1.3 OBJETIVOS GERAL E ESPECÍFICOS

Na tentativa de responder aos principais questionamentos descritos acima, esta pesquisa apresenta os seguintes objetivos geral e específicos.

1.3.1 Objetivo Geral

O objetivo principal desta pesquisa é o de descrever o processo de implementação de um sistema de Gestão de Segurança da Informação em uma Instituição Financeira de pequeno porte.

1.3.2 Objetivos Específicos

Os objetivos específicos, os quais visam auxiliar na consecução do objetivo principal, são:

a) identificar os principais componentes a serem estabelecidos em um Sistema de Gestão da Segurança da Informação;

b) identificar as etapas a serem desenvolvidas e as atividades a serem executadas na implementação de um Sistema de Gestão da Segurança da Informação em uma Instituição Financeira de pequeno porte; e

c) identificar os fatores críticos de sucesso da implementação do Sistema de Gestão de Segurança da Informação, nesta IF.

1.4 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em capítulos, sendo que este primeiro capítulo – Introdução – contém uma revisão da importância e da atualidade do tema abordado, as questões de pesquisa e os objetivos do presente trabalho. No segundo capítulo – Fundamentação Teórica – será apresentado o contexto teórico que serve como base para o estudo de caso, versando sobre os principais direcionadores da Segurança da Informação. Neste capítulo, também serão apresentados os principais modelos sobre Segurança da Informação existentes e uma análise comparativa entre estes modelos. E, finalmente, será apresentado o conteúdo esquemático da Norma *BS7799-2:2002*. O terceiro capítulo – Metodologia da Pesquisa – apresenta

as etapas segundo as quais foi desenvolvida a presente pesquisa e como foi utilizado o método de estudo de caso. O quarto capítulo – Relato do Estudo de Caso – apresenta o relato do processo de implementação do Sistema de Gestão de Segurança de Informação na empresa estudada, que pode ser descrita como uma Instituição Financeira de pequeno porte. O quinto capítulo – Modelo Resultante – busca consolidar o relacionamento entre a prática e as bases teóricas, analisando as atividades e etapas, bem como, os fatores críticos que foram identificados durante o acompanhamento e observação do processo de implementação do SGSI. Por fim, no sexto capítulo – Contribuições e Conclusões – será apresentado um resumo geral e as principais contribuições deste trabalho, tanto acadêmicas quanto práticas.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será apresentada uma revisão da literatura existente sobre a importância e relevância da informação, sobre a Gestão Estratégica da Informação, sobre os atributos da qualidade da informação e sobre a evolução do pensamento científico relativo à Segurança da Informação, destacando autores e instituições que trabalham com o tema. Será realizado um trabalho de ligação entre o referencial teórico e a situação-problema abordada nesta pesquisa, serão apresentados os principais modelos aplicados e aceitos pela legislação brasileira, além de uma análise comparativa entre estes modelos. Finalmente, serão apresentados, de maneira sintética, os componentes e elementos que constituem a *BS*7799-2:2002.

2.1 GESTÃO ESTRATÉGICA DA INFORMAÇÃO

Este item tem por objetivo apresentar como o meio acadêmico tem abordado os principais temas e conceitos relacionados à importância e à relevância da Informação, a gestão estratégica da informação, nos tempos atuais e os atributos da qualidade da informação.

O primeiro componente a ser avaliado é a importância da informação em si. Segundo Santos (2004), é a informação que possui a capacidade de agregar valor aos processos de negócio nas organizações. Uma vez reconhecido que a informação tem valor, sua boa gestão passa a ser um fator decisivo para a competitividade da empresa, principalmente ao ser considerado o clima de incerteza e turbulência em que se encontram os mercados, os quais constituem um ambiente em que os profissionais são constantemente estimulados a buscar as formas mais adequadas para a realização da gestão estratégica da informação. A tecnologia, a informação e a estratégia empresarial caminham juntas, e, sendo assim, devem ser consideradas como fontes de inovação e renovação de vantagem competitiva, e também como um fator-chave para a diferenciação de uma empresa entre suas concorrentes (MORAES; TERENCE; ESCRIVÃO F°, 2004).

Porém, antes de iniciar uma discussão sobre as formas de gestão estratégica da informação propriamente ditas, a empresa deve adotar algumas definições estratégicas, as quais, por sua vez, compõem as diversas fases da elaboração da estratégia competitiva de uma empresa, tais como: a definição e o projeto de produtos e serviços a serem oferecidos; o estabelecimento para a organização dos objetivos de desempenho financeiros e não-financeiros; a definição dos processos organizacionais e operacionais que possam atender aos objetivos de desempenho estabelecidos, diferenciando os produtos e serviços da empresa daqueles de seus concorrentes; o desenvolvimento de recursos, de tal forma que os objetivos de desempenho tenham maior probabilidade de serem alcançados; e o monitoramento do desempenho organizacional e do redirecionamento dos recursos, quando necessário (MCGEE; PRUSAK, 1994).

Uma vez que a informação e as maneiras como ela é gerenciada permeiam todas as fases da estratégia empresarial, McGee e Prusak (1994) sugerem uma estruturação, em ordem de importância, para o conjunto informacional:

a) informação na definição da estratégia, envolvendo informações atuais e precisas sobre o ambiente de mercado, as quais permitem identificar ameaças e oportunidades;

b) informação para a execução da estratégia, propiciando novas alternativas para a elaboração de processos que possam criar e oferecer produtos e serviços diferenciados; e

c) informação para retroalimentação, onde a empresa deve conseguir criar um ambiente de aprendizado constante e uma estrutura flexível, que facilmente consiga se adaptar aos objetivos definidos.

A identificação da importância da informação para a estratégia empresarial evidencia a relevância da qualidade desta informação. E os problemas relacionados à qualidade da informação incluem: valores incorretos; erros na geração desta informação; problemas técnicos com o armazenamento e o acesso aos dados; mudanças ocorridas nas necessidades informacionais dos seus usuários, entre outros. Tais imprecisões na qualidade da informação podem causar sérios impactos na satisfação do cliente, no aumento dos custos operacionais, na efetividade da tomada de decisão e na habilidade de geração e execução das estratégias organizacionais (STRONG; LEE; WANG, 1997; REDMAN, 1998).

A qualidade da informação pode ser representada por um conjunto de elementos que varia conforme o uso a ela aplicado. McGee e Prusak (1994) representam a qualidade da informação através de um conjunto de elementos: integridade, precisão, atualidade, interpretabilidade e valor geral. Em uma linha análoga de representação, Pipino, Lee e Wang (2002) apresentam a seguinte lista de elementos: economia, acessibilidade, quantidade, credibilidade, completeza, concisão, consistência, facilidade de uso, inexistência de erros, interpretabilidade, objetividade, relevância, reputação, segurança, volatilidade, entendimento.

Seguindo outra linha, Strong, Lee e Wang (1997) classificam a qualidade da informação em quatro dimensões, com diferentes elementos dentro de cada uma destas dimensões. A dimensão de “qualidade intrínseca” contém os elementos “acurácia”, “objetividade”, “credibilidade” e “reputação”. A dimensão de “acesso aos dados” contém os elementos “acessibilidade” e “segurança”. A dimensão “contextual” contém os elementos “relevância”, “valor”, “temporalidade” e “completeza e quantidade”. A dimensão “representatividade” contém os elementos “interpretabilidade”, “facilidade de entendimento”, “representação concisa e consistente”. Outros autores também classificam a qualidade da informação em dimensões, agrupando conjuntos de elementos, tais como a dimensão “tempo” (com os elementos “volatilidade”, “atualidade”, “freqüência” e “amplitude”), a dimensão “conteúdo” (com “acurácia”, “relevância”, “completeza”, “consistência”, “escopo” e “performance”) e a dimensão “formato” (com “claridade”, “detalhe”, “ordem”, “apresentação” e “mídia”).

Porém, independentemente da forma de representação, tanto da qualidade da informação quanto de sua forma de gestão, a questão da “segurança” da informação surge quase como uma constante. E isto pode ser principalmente observado quando aplicado às normas e regras internacionais relacionadas ao tema.

Williams (2001) salienta que o conceito de segurança aplica-se a toda e qualquer informação. “Segurança” diz respeito à proteção de recursos valiosos contra a sua perda, divulgação imprópria ou dano. “Recursos valiosos” são os dados ou informações gravadas em, processadas por, armazenadas em, compartilhadas por, transmitidas ou recuperadas de um meio magnético. Dados (ou informações) precisam estar protegidos contra danos causados por ameaças que possam levar à sua perda, impossibilidade de acessibilidade, alteração ou divulgação indevida. A

segurança precisa ser lidada de uma forma pró-ativa e rápida para que sua aplicação seja eficiente.

Williams (2001) e o *British Standard Institute* (BSI) afirmam que o objetivo da segurança da informação é o de proteger os interesses daqueles que confiam nas informações e nos sistemas, meios e métodos de comunicação que disponibilizam esta informação contra danos resultantes de falhas de indisponibilidade, confidencialidade e integridade. Estes são os objetivos, as dimensões mais relevantes e os paradigmas a serem considerados na segurança da informação, e serão alcançados quando:

a) os sistemas de informação estiverem disponíveis e prontos para o uso quando requisitados, e puderem apropriadamente resistir a ataques e recuperar-se de falhas (características de disponibilidade);

b) os dados e informações forem divulgados apenas àqueles que têm direito e autoridade de conhecê-las (características de confidencialidade);

c) os dados e informações forem protegidos contra modificações não autorizadas (características de integridade); e

d) com relação às transações comerciais, os dados e informações puderem ser confiáveis (características de autenticidade e de não-repúdio).

Uma vez definidos os objetivos, surge a necessidade de identificar quais as atividades envolvidas na segurança da informação. De acordo com o *Managing Security of Information* da *International Federation of Accountants*, de 1998, existem seis principais atividades a serem realizadas, envolvendo a segurança da informação, com o objetivo de desenvolver e manter controles adequados, de acordo com princípios geralmente aceitos, utilizando-se para isto uma abordagem dinâmica e integrada. Estas seis atividades são as seguintes:

a) desenvolvimento de políticas: os objetivos de segurança e princípios da organização fornecem uma estrutura básica para a primeira etapa crítica, relacionada à gestão da segurança da informação, para que seja desenvolvida uma política de segurança para toda a organização;

b) papéis e responsabilidades: para que a segurança seja eficaz, é obrigatório que os papéis, as responsabilidades, e as autoridades individuais sejam claramente comunicadas e compreendidas por todos;

c) projeto: uma vez que uma política tenha sido aprovada pela Alta Administração[4] da organização, e os papéis e as responsabilidades relacionadas forem atribuídos, é necessário desenvolver uma estrutura de segurança e de controle que consista em padrões, medidas, práticas e procedimentos;

d) execução: após os projetos dos padrões da segurança, medidas, práticas, e procedimentos terem sido aprovados, a solução deve ser implementada em tempo hábil, e mantida a partir de então;

e) monitoração: deve ser estabelecida a mensuração de medidas para detectar e assegurar a correção de brechas na segurança, de forma que todas as brechas reais ou suspeitadas possam ser prontamente identificadas, investigadas e tratadas, para assegurar conformidade com as políticas, padrões, e práticas aceitáveis de segurança adotados naquele período; e

f) consciência, treinamento, e instrução: para o sucesso do programa da segurança de uma organização, é de importância crítica que haja a consciência da necessidade de proteger a informação, de treinamento nas habilidades necessárias para operar com segurança os sistemas de informação, e de instrução em medidas e práticas de segurança.

2.2 SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA TI

A questão da segurança da informação no âmbito da TI ganhou força com o surgimento dos computadores de tempo compartilhado, na década de 1960, que possibilitavam que mais de uma pessoa fizessem uso simultâneo de um mesmo computador. Atualmente, isto é muito comum, mas, até então, não era algo possível. O tempo compartilhado possibilitou que vários usuários pudessem acessar o mesmo computador e, conseqüentemente, as mesmas informações. No entanto, este

[4] Alta Administração: O termo original, em inglês, empregado na norma é *Management*, que significa Administração ou Gerenciamento. No Brasil, a tradução mais usualmente utilizada, no contexto da Segurança da Informação, é a de “Alta Administração”, representando o mais alto escalão da empresa. (nota do autor)

acesso poderia gerar efeitos indesejáveis. Tal problema ficou caracterizado como o "problema clássico dos computadores". À época, perguntava-se: como fazer com que usuários autorizados ao uso do computador possam ter acesso a determinadas informações, ao mesmo tempo em que os usuários não autorizados não possam acessá-las?

Em resposta a este problema, em outubro de 1967, foi criada, no Departamento de Defesa dos Estados Unidos (*DoD*) uma força-tarefa, que, definiu e publicou o documento *Security Control for Computer System: Report of Defense Science Boad Task Force on Computer Security* (editado por W. H. Ware) considerado o primeiro processo oficial de criação de um conjunto de regras para segurança da informação em computadores.

Em outubro de 1972, J. P. Anderson escreveu um relatório técnico denominado: *Computer Security Technologs Planning Study* no qual descreve, sob seu ponto de vista, todos os problemas envolvidos no processo de fornecimento de mecanismos necessários para salvaguardar a segurança dos computadores.

Este documento, combinado com os materiais produzidos por D. E. Bell e por L. J. La Padula, denominados *Secure Computer Systems – Mathematical Fundations*, *Mathematical Model* e *Refinament of Mathematical Model*, deram origem ao que ficou conhecido como *Doutrine*, e que tornou-se a base para a maioria dos trabalhos posteriores, elaborados na área de segurança da informação.

Em 1977, o *DoD* formulou um plano sistemático para tratar o problema clássico dos computadores, o qual daria origem ao *DoD-Computer Security Initiative*. Este documento resultou na criação de um Centro para avaliar o quão seguras eram as soluções computacionais criadas no âmbito do *DoD*. A implementação deste Centro gerou a necessidade de criação de um conjunto de regras a serem utilizadas no processo de avaliação das soluções computacionais. Este conjunto de regras é conhecido como *The Orange Book*. O primeiro diretor do Centro foi o Cel. Roger R. Schell.

O processo de redação do *Orange Book*, conhecido oficialmente como *Trusted Computer Evaluation Criteria – DoD5200.28-STD*, foi iniciado em 1978, sendo que, no mesmo ano, foi publicada a sua primeira versão preliminar. Entretanto, a versão final do documento somente foi publicada em 26/12/1985.

Graças às operações e ao processo de criação do Centro de Avaliação do *DoD* e do *Orange Book*, foi possível a produção de uma grande quantidade de

documento técnicos, que representaram o primeiro passo para a formulação de uma norma coesa e completa sobre a segurança em computadores. A série de documentos originados do esforço conjunto dos membros do Centro é reconhecida pelo nome de: *The Rainbow Series* cujos documentos continuam sendo atualizados até a presente data (GONÇALVES, 2000).

O *Orange Book* representou o "marco zero" a partir do qual foram elaborados vários padrões de segurança, cada qual com sua filosofia e métodos proprietários. Contudo, visando uma padronização mundial, foi iniciado um esforço para a construção de uma norma que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação.

Este esforço foi liderado pela *International Organization for Standardization* (*ISO*). As primeiras abordagens da *ISO* quanto à segurança da Informação surgiram com as normas *ISO*7948-2 e a ISO15408. A *ISO*7948-2 descreve os mecanismos e procedimentos de segurança associados ao modelo de referência *Open Systems Interconnection* (*OSI*) empregado no desenvolvimento de sistemas de comunicação em redes. A *ISO15408*, mais conhecida como *Common Criteria*, foi homologada em 1999, por uma associação de organizações americanas, a *National Institute of Standards and Technology* (*NIST*) e *National Security Agency* (*NSA*), e os governos dos países Canadá, França, Holanda, Alemanha e Inglaterra, com os objetivos de identificar e avaliar facilidades de segurança para computadores e sistemas, e também de subsidiar os desenvolvedores destes sistemas (SANTILLO, 2001).

No Reino Unido, os primeiros passos na área da segurança da informação remontam ao ano de 1987. Neste ano, o Departamento de Comércio e Indústria do Reino Unido (*DTI*) criou um centro de segurança de informações, o *Commercial Computer Security Center* (*CCSC*), que, dentre suas atribuições, possuía a tarefa de criar um código de segurança para os usuários das informações, por meio da criação de critérios de avaliação da segurança (SOLMS, 1998). O trabalho do *CCSC* resultou, em 1990, na primeira versão de um código de segurança, denominado PD0003 – *Code to Information Security Management*.

Em 1993, o *British Standard Institute* (*BSI*) criou um grupo de trabalho com os objetivos de estabelecer um código de práticas para promover o planejamento de segurança da informação para o mundo comercial e de subsidiar empresas na elaboração de políticas de segurança (ROBIETTE, 2003). Com base no trabalho realizado pelo *CCSC*, o PD0003 foi revisado pelo grupo do *BS*I, e, em 1995, foi

publicado sob a forma de norma com o nome de *BS*7799:1995. Uma segunda parte foi publicada em 1998, sob o nome de *BS*7799-2:1998, e, após uma significativa revisão, foram novamente publicadas em 1999, respectivamente sob os nomes de *BS*7799-1:1999 e *BS*7799-2:1999 (SOLMS, 1998; COBB, 2001; HEFFERAN, 2000).

Ao longo de seu desenvolvimento, a *BS7799* foi sendo adotada não apenas pela Inglaterra, mas também por outros países da comunidade Britânica, tal como Austrália, África do Sul e Nova Zelândia (SOLMS, 1998). Através de uma associação entre o *Information Technology Committee*, da *ISO*, e a *International Electro-Technical Commission* (*IEC*), em dezembro de 2000, a norma *BS*7799 foi aprovada em regime de *fast-track* (aprovação sumária), sendo homologada e publicada com o nome de *ISO*/*IEC*17799:2000, tornando-se uma norma internacional (MODULO, 2001). Com a homologação da *ISO*/*IEC*17799:2000 pela *ISO*/*IEC*, a Associação Brasileira de Normas Técnicas (ABNT) homologou, em 2001, a norma Brasileira de Segurança da Informação, denominada NBR ISO/IEC17799:2001, sendo esta a primeira versão da norma em língua portuguesa. Em setembro de 2002, foi publicada a *BS*7799-2:2002 pelo BSI, e, em 2005, foi publicada, a norma correspondente, a *ISO*/*IEC*17799:2005 pela ISO/IEC. Em janeiro de 2006, a Norma *ISO/IEC*17799-2:2005 foi publicada pela *ISO/IEC*, e renomeada com o número *ISO*27001.

Com o objetivo de facilitar o entendimento das normas envolvidas, pode ser analisado o Quadro 1:

NORMA	OBSERVAÇÃO
*BS*7799:1995	1ª versão
*BS*7799-2:1998	1ª versão
*BS*7799-1:1999 e *BS*7799-2:1999	Revisão das anteriores
ISO/*IEC*17799:2000 ou *BS*7799-1:2000	Revisão da *BS*7799-1:1999
*BS*7799-2:2002	Revisão da *BS*7799-2:1999
ISO/*IEC*17799:2005	Revisão da *ISO*/*IEC*17799:2000
ISO/*IEC*17799-2:2005	Revisão da BS7799-2:2002 (*ISO*27001)

Quadro 1 – Normas relacionadas à Segurança da Informação

Fonte: o autor.

A presente pesquisa usa como referencial a norma *BS*7799-2:2002 - Sistemas de Gestão de Segurança da Informação – especificações com guia de uso que introduz os fundamentos para auditoria de conformidade por terceiros

(certificação) e foi revisada para se harmonizar com outras normas de sistemas de Gestão, tais como, a *ISO*9001 e a *ISO*14001. Esta norma utiliza o modelo de processo *Plan-Do-Check-Act* (*PDCA*) como parte integrante do sistema de Gestão para a abordagem, desenvolvimento, implementação e melhoria, de uma maneira eficiente, de um Sistema de Gerenciamento de Segurança da Informação (SGSI) na organização, abrangendo os riscos de negócio, no seu contexto total. Como norma de apoio, também será referenciada a norma *ISO*/*IEC*17799:2000, que provê um guia de recomendações para os itens de controle de Segurança da Informação a serem implantados A *ISO*/*IEC*17799:2000 foi revisada pelo grupo de trabalho *ISO*/*IEC*-SC27, composto por delegados de mais de 24 países. O autor da presente dissertação fez parte da delegação brasileira de revisão que, em outubro de 2004, em Fortaleza-CE, no Brasil, concluiu esta revisão. Como parte de suas atividades na delegação, o autor apresentou duas palestras sobre sua experiência de implementação da *BS*7799-2:2002 para o citado grupo de trabalho e convidados. A primeira das palestras foi realizada na Instituição Financeira patrocinadora do evento, em Fortaleza, e, no dia seguinte, a segunda palestra ligada ao tema da Segurança da Informação foi apresentada, em São Paulo, em outra instituição. A *ISO*/*IEC1*7799:2005 é fruto do trabalho deste grupo de delegados, e foi publicada no segundo semestre de 2005.

2.3 MODELOS APLICADOS

Conforme foi citado anteriormente, para incrementar o nível da segurança da informação nas organizações, foram desenvolvidos vários modelos aplicados, alguns dos quais ainda são atualmente adotados. A seguir, serão apresentadas as práticas mais relevantes e uma avaliação comparativa entre elas.

2.3.1 Information Tecnology Infrastructure Library – ITIL

O *ITIL* é o modelo de referência para gerenciamento de processos de TI mais aceito mundialmente. A metodologia foi criada pela Secretaria de Comércio (*Office of Government Commerce, OGC*) do governo da Inglaterra, a partir de pesquisas realizadas junto a diversos especialistas da área de TI, com o objetivo definir as melhores práticas para a gestão da área de TI nas empresas privadas e públicas. Este trabalho resultou na norma *BS*15000, sendo esta um anexo da *ISO*9000:2000. O foco do modelo está em descrever os processos necessários para gerenciar eficiente e eficazmente a infra-estrutura de TI, de modo a garantir os níveis de serviço (*SLAs*) acordados com os clientes internos e externos. Na Figura 1 é apresentado um diagrama das principais práticas e áreas de interesse abordadas pelo *ITIL*.

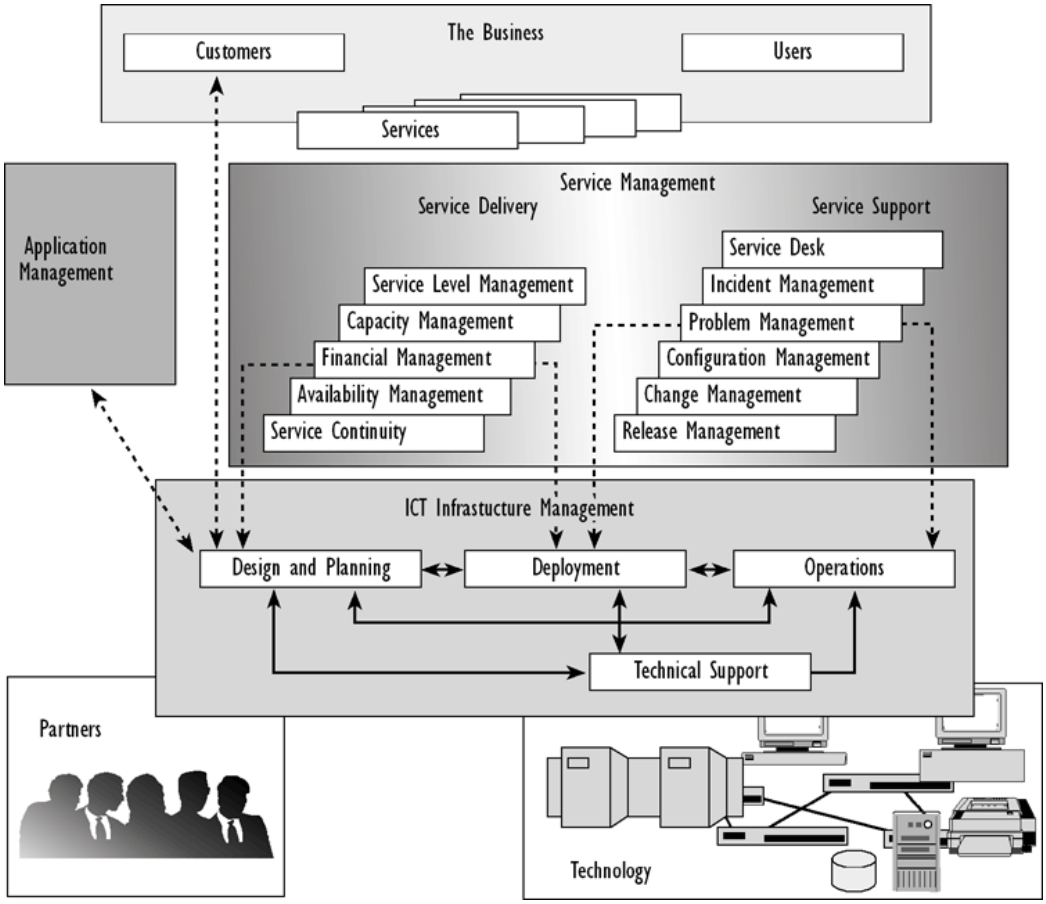

Figura 1 – Diagrama esquemático do ITIL

Fonte: Brodbeck (2004).

2.3.2 Control Objectives for Information and related Tecnology – COBIT

O *COBIT* é uma estrutura de relações e processos desenvolvida com o objetivo de dirigir e controlar o ambiente de TI, para que as metas da organização possam ser alcançadas com a agregação de valor, ao mesmo tempo em que se equilibra risco *versus* retorno sobre o investimento em TI e seus processos (*IT Governance Institute*, 2005). O *COBIT* é dividido em quatro domínios, ou áreas de interesse, onde são agrupados os 34 processos a serem implementados. A Figura 2 apresenta um diagrama com as principais práticas abordadas pelo *COBIT*.

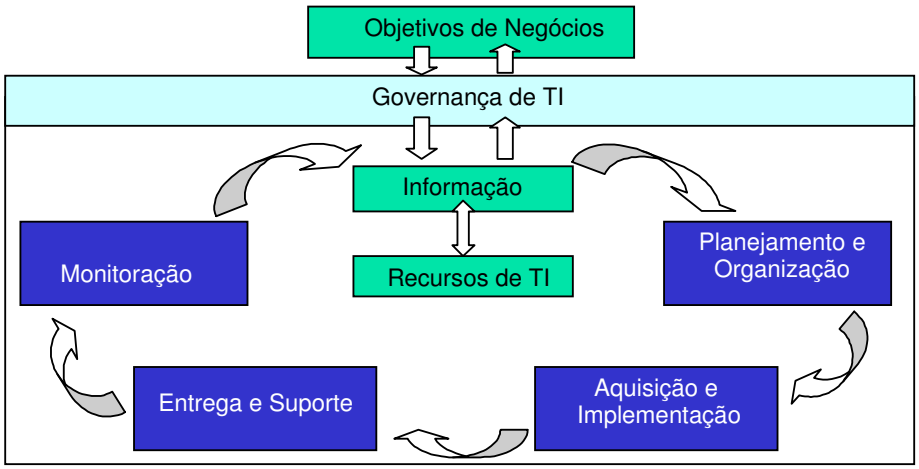

Figura 2 – Diagrama esquemático do COBIT

Fonte: Brodbeck (2004).

Considerando os domínios do *COBIT*, estão descritos no Quadro 2 os processos definidos neste modelo.

DOMÍNIOS	PROCESSO
Planejamento e Organização	
	1 Define o Plano Estratégico de TI
	2 Define a Arquitetura da Informação
	3 Determina a Direção Tecnológica
	4 Define a Organização de TI e seus
	5 Gestão de Investimentos em TI
	6 Gestão da Comunicação das Direções de TI
	7 Gestão de Recursos Humanos
	8 Assegura alinhamento de TI com os
	9 Avaliação de Riscos
	10 Gestão de Projetos
	11 Gestão da Qualidade
Aquisição e Implementação	
	1 Identifica as Soluções de Automação
	2 Adquire e Mantém Aplicativos
	3 Adquire e Mantém Infra-estrutura Tecnológica
	4 Desenvolve e Mantém Procedimentos
	5 Instalação e Aceitação de Sistemas
	6 Gestão de Mudanças
Entrega e Suporte	
	1 Define e Mantém Níveis de Serviço
	2 Gestão de Serviços Terceirizados
	3 Gestão de Performance e Capacidade
	4 Garantia de Continuidade de Negócios
	5 Garantia de Segurança de Sistemas
	6 Identifica e Aloca Custos
	7 Educa e Treina Usuários
	8 Assiste e dá Suporte a Usuários
	9 Gestão de Configuração
	10 Gestão de Problemas e Incidentes
	11 Gestão de Dados
	12 Gestão de Infra-estrutura
	13 Gestão de Operações
Monitoração	
	1 Monitora Processos
	2 Avalia a adequação dos Controles Internos
	3 Provê Auditoria Independente
	4 Provê Segurança Independente

Quadro 2 – Dimensões e Processos do COBIT

Fonte: o autor.

2.3.3 Segurança da Informação – ISO/IEC17799:2000 e BS7799-2:2002

Conforme apresentado em itens anteriores e detalhado no Anexo D, as normas de Segurança da Informação são divididas em duas partes, sendo que a primeira parte (norma *ISO*/*IEC*17799:2000) determina, para cada uma das áreas de risco da organização, quais os itens a serem controlados. Já a segunda parte (norma *BS*7799-2:2002) trata dos processos que devem ser desenvolvidos para a implementação de um SGSI. Os quadros 3 e 4 apresentam, de forma esquemática, os principais elementos das referidas normas:

ELEMENTOS
1 – Escopo na Norma
2 – Termos e Definições
3 – Política de Segurança
4 – Segurança Organizacional
5 – Classificação e Controle de Ativos de Informação
6 – Segurança em Pessoas
7 – Segurança Física e do Ambiente
8 – Gestão de Operações e Comunicações
9 – Controle de Acesso
10 – Desenvolvimento e Manutenção de Sistemas
11 – Gestão de Continuidade do Negócio
12 – Conformidade

Quadro 3 – Elementos da Norma ISO/IEC17799:2000

Fonte: o autor.

ELEMENTOS
1 – Escopo
2 – Referências Normativas
3 – Termos e Definições
4 – Sistema de Gestão de Segurança da Informação
5 – Responsabilidade da Alta Administração
6 – Análise Crítica do SGSI
7 – Melhoria do SGSI

Quadro 4 – Elementos da Norma BS7799-2:2002

Fonte: o autor.

2.3.4 Análise Comparativa

Segundo a *ISACA* (2004), os três modelos apresentam, em resumo, as seguintes características:

a) *ITIL* – é um modelo focado no detalhamento de processos de infra-estrutura de TI a serem implementados, porém limitado, tanto em segurança quanto no desenvolvimento de sistemas;

b) *COBIT* – é um modelo focado no estabelecimento dos controles a serem utilizados na área de TI e de suas métricas, mas não apresenta os fluxos de processos envolvidos (o "como fazer") e não é suficientemente abrangente quanto aos requisitos da segurança; e

c) *ISO/IEC*17799 e *BS*7799-2:2002 – a primeira, é focada no estabelecimento dos controles de segurança, e a segunda, nos processos de gestão da segurança a serem implementados, mas também não apresentam os fluxos de processos envolvidos.

Considerando as definições apresentadas anteriormente, verifica-se que as práticas atualmente adotadas dão significativa importância à área de Tecnologia da Informação (TI) como elemento de convergência das informações e como ponto focal das iniciativas. Apesar de se constituir em um corpo de conhecimento relevante, o *ITIL* está focado na infra-estrutura de TI, tornando sua atuação mais objetiva, e conseqüentemente, mais restrita. O *COBIT* também possui origem na área de TI, no entanto, é um modelo mais abrangente, uma vez que também considera os problemas de Segurança de Tecnologia da Informação e seus relacionamentos. A *BS*7799-2:2002, por sua vez, estabelece um modelo de Gestão da Segurança da Informação onde a área de TI é um dos componentes mais relevantes, porém não é o único a ser considerado.

Implementar um modelo de Gestão da Segurança da Informação em uma organização significa implementar uma sistemática abrangente, integrada e contínua, para minimizar riscos associados ao tratamento da informação em qualquer uma de suas áreas. A *BS*7799-2:2002 é um modelo de gestão que foi estabelecido buscando o mesmo formato e sistemática das normas *ISO*9001 (que trata de Gestão da Qualidade) e *ISO*14000 (que trata da Gestão Ambiental) e, desta

forma, possibilitam que auditores independentes, devidamente credenciados, possam certificar a conformidade da sistemática implementada com o que está estabelecido nas respectivas normas. A similitude de estrutura entre a norma *BS779-2:2002* e as das demais práticas de Gestão foi o que possibilitou que esta norma fosse adotada pela *ISO* e renomeada para *ISO*27001.

2.4 NORMA *BS*7799-2:2002

Neste item será apresentada, de forma resumida[5], a transcrição dos elementos e componentes da Norma *BS*7799-2:2002 que foram utilizados na operacionalização da pesquisa. Este item também visa apresentar ao leitor os principais conceitos estabelecidos e as práticas adotadas na implementação do Sistema de Gestão da Segurança da Informação que foram utilizados pelo pesquisador na condução do trabalho.

Norma BS7799-2:2002

CAPÍTULO 0 – Introdução

0.1 Geral – trata da decisão estratégica da empresa ao adotar um SGSI;

0.2 Abordagem – identifica a necessidade de a organização atender a quatro requisitos básicos: (a) entender os requisitos de segurança da empresa; (b) implementar e operar controles; (c) monitorar e revisar o desempenho do sistema; e (d) melhorar continuamente (o SGSI);

O atendimento destes requisitos básicos deve ser baseado no ciclo *PDCA* (*Plan*, *Do*, *Check*, *Act*) estabelecido por Deming (2002) na norma BS7799-2:2002. O item “a”, acima, corresponde ao *Plan*, o item “b” corresponde ao *Do*, o item “c” ao

[5] A numeração utilizada, neste item, para a identificação dos capítulos e componentes da norma BS7799-2:2002 é a mesma utilizada na própria norma, com o objetivo de manter a correspondência com o documento original. Os nomes dos autores e documentos citados também fazem parte da própria norma (nota do autor).

Check e, finalmente, o item “d” corresponde ao *Act*. A seguir, é apresentado um diagrama esquemático do *PDCA*, relacionado ao SGSI.

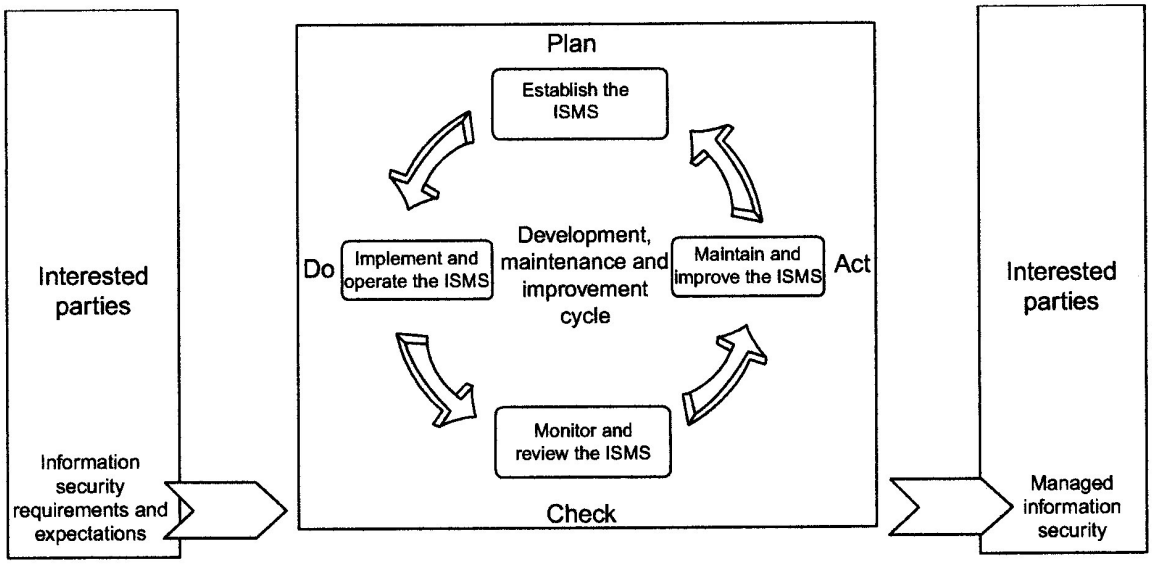

Figura 3 – Ciclo PDCA para o SGSI
Fonte: British (2002).

CAPÍTULO 1 – Escopo

1.1 Escopo geral da norma – trata dos requisitos a serem considerados para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um SGSI.

1.2 Aplicação da norma – determina que os requisitos apresentados sejam genéricos para implantação em qualquer organização, independentemente de seu tipo, tamanho e natureza do negócio. Quando algum dos requisitos da norma não puder ser aplicado, devido à natureza da organização e de seu negócio, pode ser considerada a exclusão do requisito. Quando houver exclusões, as mesmas somente serão aceitas se tais exclusões não afetarem a habilidade de a organização, e/ou sua responsabilidade prover a Segurança da Informação. Não é aceita a exclusão de qualquer requisito especificado nos Capítulos 4, 5, 6 e 7.

CAPÍTULO 2 – Referências Normativas

Cita os seguintes documentos de referência como indispensáveis para a aplicação da norma. Para referências temporais, somente se aplica a edição citada.

Para referências não-temporais, se aplica a última edição dos documentos referenciados: (a) EN *ISO*9001:2000, *Quality management systems – Requirements*; (b) *ISO*/*IEC*17799:2000, *Information technology – Code of practice for information security management*; e (c) *ISO Guide* 73:2002, *Risk management – Vocabulary – Guidelines for use in Standards*.

CAPÍTULO 3 – Termos e definições

Para os objetivos da norma, são aplicados os seguintes termos e definições:

3.1 Disponibilidade – garantir que usuários autorizados tenham acesso às informações e ativos associados, quando necessário (*ISO*/*IEC*17799:2000);

3.2 Confidencialidade – garantir que a informação é acessível somente a quem é autorizado a ter acesso (*ISO*/*IEC*17799:2000);

3.3 Segurança da Informação – preservação da segurança em relação à confidencialidade, à integridade e à disponibilidade da informação;

3.4 Sistema de Gestão da Segurança da Informação (SGSI) – é parte de todo o sistema de gestão, baseado na abordagem do risco ao negócio, e visa estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação;

3.5 Integridade – salvaguardar a acurácia e completeza da informação e métodos de processamento (*ISO*/*IEC*17799:2000);

3.6 Aceitação de risco – decisão de aceitar um risco (*ISO Guide* 73);

3.7 Análise de risco – uso sistemático da informação para identificar fontes de risco e estimar o risco (*ISO Guide* 73);

3.8 Avaliação de risco – processo geral de análise de risco e parametrização do risco (*ISO Guide* 73);

3.9 Parametrização de risco – processo de comparação entre a estimativa de risco e um dado critério de risco que determine a significância deste risco (*ISO Guide* 73);

3.10 Gerenciamento de risco – atividades coordenadas para direcionar e controlar uma organização em relação ao risco (*ISO Guide* 73);

3.11 Tratamento de risco – processo de tratamento de seleção e implementação de medidas para modificar riscos (*ISO Guide* 73); e

3.12 Declaração de Aplicabilidade – documento que descreve os objetivos dos controles e os controles que são relevantes e aplicáveis ao SGSI da organização, baseado nos resultados e conclusões dos processos de estimativa e tratamento de risco.

CAPÍTULO 4 – Sistema de Gestão da Segurança da Informação – SGSI

4.1 Requisitos Gerais – determina que a organização deva desenvolver, implementar, manter e melhorar continuamente o SGSI, de acordo com as atividades de negócio e riscos da organização.

4.2 Estabelecendo e administrando o SGSI – no estabelecimento do SGSI, a organização deve atender aos seguintes aspectos: (a) definir o escopo do SGSI, considerando as características do negócio, a organização, sua localização, ativos e tecnologia; (b) estabelecer a política do SGSI, considerando as características do negócio, a organização, sua localização, ativos e tecnologia e aprovar pela alta administração; (c) definir uma abordagem sistemática de avaliação de risco; (d) identificar os riscos; (e) avaliar estes riscos; (f) identificar e avaliar opções para tratamento dos riscos; (g) selecionar tanto os objetivos dos controles quanto estes controles para tratamento dos riscos; (h) preparar uma declaração de aplicabilidade; e (i) obter a aprovação da Alta Administração para os riscos residuais e autorização para implementação e operação do SGSI.

4.2.1 Implementação e Operação do SGSI – devem ser consideradas as seguintes etapas: (a) formular um plano de tratamento do risco que identifique as ações, responsabilidades e prioridades; (b) implementar o plano de tratamento do risco; (c) implementar os controles selecionados; (d) implementar um programa de treinamento e conscientização; (e) gerenciar operações; (f) gerenciar recursos; e (g) implementar procedimentos e outros controles capazes de habilitar a pronta detecção e respostas a incidentes de segurança.

4.2.2 Analisar Criticamente e Monitorar o SGSI – a organização deve considerar as seguintes etapas: (a) executar procedimentos de monitoramento para detectar prontamente erros, identificar brechas e incidentes de segurança bem ou mal sucedidos, habilitar gerenciamento de

atividades e responsabilidades, determinar as ações a serem tomadas para solucionar brechas de segurança; (b) responsabilizar-se por revisões regulares da efetividade do SGSI; (c) analisar criticamente os níveis de risco residual e de risco aceitável; (d) conduzir auditorias internas do SGSI em intervalos planejados; (e) responsabilizar-se pela realização de análises críticas do SGSI, feita pela Alta Administração; e (f) registrar ações e eventos que possam impactar na efetividade ou desempenho do SGSI.

4.2.3 Manutenção e Melhoria do SGSI – devem ser considerados os seguintes aspectos: (a) implementar e identificar melhorias no SGSI; (b) tomar ações corretivas e preventivas apropriadas; (c) comunicar os resultados e ações, e estabelecer acordos com as partes envolvidas; e (d) garantir que as melhorias implementadas auxiliem no atendimento dos objetivos.

4.3 Requisitos de Documentação – Este item determina quais os documentos devem ser gerados para a formalização do SGSI: (a) declaração documentada da Política de Segurança e dos objetivos dos controles; (b) escopo do SGSI, os procedimentos e controles que sustentam o SGSI; (c) relatório de avaliação de risco; (d) plano de Tratamento de Risco; (e) procedimentos documentados que sejam necessários à organização e que garantam a efetividade do planejamento, operação e controle dos processos de segurança da informação; (f) registros requeridos pela norma; e (g) declaração de Aplicabilidade.

Este item determina de que forma os documentos devem ser controlados: (a) aprovar documentos para adequação prévia ao assunto; (b) revisar, atualizar e re-aprovar documentos, quando necessário; (c) garantir que sejam identificadas as mudanças feitas e qual o status da versão atualmente em uso destes documentos; (d) garantir que as versões mais recentes dos documentos relevantes estejam disponíveis nos locais de uso; (e) garantir que os documentos sejam legíveis e prontamente identificáveis; (f) garantir que sejam identificados os documentos de origem externa; (g) garantir que seja controlada a distribuição dos documentos; (h) prevenir o uso não-intencional de documentos obsoletos; e (i) aplicar identificação adequada, caso estes documentos devam ser mantidos por algum propósito.

Este item também determina quais registros devem ser estabelecidos e mantidos para prover evidências de conformidade com os requisitos e com a efetividade operacional do SGSI. Estes registros devem ser controlados. O SGSI

deve considerar qualquer requisito legal relevante. Tais registros devem ser estabelecidos e mantidos para prover evidências de conformidade com os requisitos e com a efetividade operacional do SGSI. Os registros devem permanecer legíveis, prontamente identificáveis e recuperáveis. Os controles necessários para identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição dos registros devem ser documentados. Deve existir um processo de gerenciamento para determinar a necessidade de extensão destes registros.

CAPÍTULO 5 - Responsabilidade da Alta Administração

5.1 Comprometimento da Alta Administração com o SGSI – a Alta Administração deve prover evidências do seu comprometimento no estabelecimento, implementação, operacionalização, monitoramento, revisão, manutenção e melhoraria do SGSI: (a) estabelecendo uma política de segurança da informação; (b) garantindo que os planos e objetivos de segurança da informação são estabelecidos; (c) estabelecendo papéis e responsabilidades para a segurança da informação; (d) comunicando a organização sobre a importância de atender aos objetivos de segurança da informação e da conformidade com a política de segurança da informação, sobre suas responsabilidades perante as leis e sobre a necessidade da melhoria contínua neste sistema; (e) provendo recursos suficientes para desenvolver, implementar, operar e manter o SGSI; (f) decidindo o nível de risco aceitável; e (g) conduzindo análises críticas do SGSI.

5.2 Gerenciamento de recursos – a organização deverá prover os recursos necessários para: (a) estabelecer, implementar, operar e manter um SGSI; (b) garantir que os procedimentos de Segurança de Informação suportem os requisitos do negócio; (c) identificar e endereçar os requisitos legais e reguladores, bem como as obrigações contratuais de segurança; (d) manter a segurança adequada através da correta aplicação de todos os controles implementados; (e) executar revisões, quando necessário, e reagir de acordo com os resultados destas revisões; e (f) onde requerido, melhorar a efetividade do SGSI.

A organização deve garantir que todo o pessoal que tem responsabilidades definidas no SGSI seja competente para executar as tarefas requeridas: (a) determinando as competências necessárias para que as pessoas executem suas tarefas de acordo com o SGSI; (b) provendo treinamento adequado e, se necessário,

empregar pessoal competente para satisfazer estas necessidades; (c) avaliando a efetividade dos treinamentos fornecidos e das ações tomadas; e (d) mantendo registros de educação, treinamento, habilidade, experiência e qualificações.

CAPÍTULO 6 – Revisão do SGSI pela Alta Administração

6.1 Revisão Geral – a Alta Administração deve revisar o SGSI em intervalos planejados, para garantir sua aplicabilidade contínua, sua adequação e efetividade. Esta revisão deve incluir avaliação de oportunidades para melhoria e necessidades de mudança do SGSI, incluindo a sua política e seus objetivos de segurança. Os resultados das revisões devem ser claramente documentados e devem ser mantidos registros destas revisões.

6.2 Entrada para análise – os seguintes dados devem ser considerados como entradas para uma análise crítica do SGSI: (a) resultados das auditorias e análises do SGSI; (b) retroalimentação e sugestões das partes interessadas; (c) técnicas, produtos ou procedimentos que possam ser utilizados pela organização para aprimorar a performance e a efetividade do SGSI; (d) dados representativos da situação atual das ações corretivas e preventivas implementadas; (e) vulnerabilidades ou ameaças não adequadamente endereçadas na estimativa de risco anterior; (f) ações de acompanhamento das análises críticas anteriores; (g) qualquer mudança que possa afetar o SGSI; e (h) recomendações para melhoria.

6.3 Saídas da análise – os dados de saída da análise crítica da Alta Administração devem incluir quaisquer decisões e ações relacionadas aos seguintes aspectos: (a) melhoria da efetividade do SGSI; (b) modificação dos procedimentos que afetam a segurança da informação, quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI; e (c) recursos necessários.

6.4 Auditorias Internas do SGSI – a organização deve conduzir auditorias internas do SGSI em intervalos planejados para determinar se os objetivos dos controles, os próprios controles, os processos e os procedimentos do SGSI: (a) estão em conformidade com os requisitos desta norma, regulamentos e legislação relevantes; (b) estão em conformidade com os requisitos de segurança da informação identificados; (c) são efetivamente implementados e mantidos; e (d) são executados conforme as expectativas previamente formuladas, relativas a eles.

Um programa de auditoria deve ser planejado levando em consideração a situação e a importância dos processos e áreas a serem auditadas, bem como o resultado de auditorias anteriores. Devem ser definidos os critérios de auditoria, escopo, freqüência e métodos. A seleção de auditores e a condução das auditorias devem garantir a objetividade e imparcialidade do processo de auditoria. As responsabilidades e requisitos para o planejamento e condução de auditorias, elaboração dos relatórios com os seus resultados e manutenção dos registros relativos a eles devem ser definidos em um procedimento documentado.

CAPÍTULO 7 - Melhoria do SGSI

7.1 Melhoria Contínua – a organização deve melhorar continuamente a efetividade do SGSI através do uso da Política de Segurança da Informação, Objetivos de Segurança, resultados de auditoria, análise de eventos monitorados, ações preventivas e corretivas e revisão dos gestores.

A principal característica de um SGSI é sua capacidade de melhoria contínua. Esta melhoria deve ser baseada em ações tomadas frente a problemas e incidentes detectados. A capacidade de estabilização do SGSI, tanto em relação ao nível de segurança quanto ao nível de aceitabilidade, é fortemente relacionada à velocidade com que estes problemas são detectados e as melhorias são efetivadas.

7.2 Ação Corretiva – a organização deve agir para eliminar a causa de não-conformidades associadas à implementação e operação do SGSI, de forma a prevenir a repetição de sua ocorrência. Os procedimentos documentados para a ação corretiva devem definir requisitos para: (a) identificar as não-conformidades detectadas na implementação e/ou operação do SGSI; (b) determinar as causas destas não-conformidades; (c) avaliar a necessidade de ações para garantir que as não-conformidades não ocorram novamente; (d) determinar e implementar as ações corretivas necessárias; (e) registrar os resultados das ações tomadas; e (f) revisar as ações corretivas tomadas.

As ações corretivas a serem implementadas devem ser focadas em problemas detectados no processo, como por exemplo, o não-atendimento de normas, os erros na execução de procedimentos e as falhas na estrutura de segurança, conforme padrão definido.

7.3 Ações Preventivas – a organização deve determinar ações para se proteger em relação a futuras não-conformidades, de forma a prevenir sua ocorrência. Ações preventivas tomadas devem ser apropriadas ao impacto dos problemas potenciais. Um procedimento documentado para ação preventiva deve definir requisitos para: (a) identificar potenciais não-conformidades e suas causas; (b) determinar e implementar ações preventivas necessárias; (c) registrar os resultados das ações tomadas; (d) revisar as ações preventivas tomadas; e (e) identificar mudanças nos riscos e garantir que a atenção esteja focada em mudanças que apresentem riscos mais significativos.

3. METODOLOGIA DE PESQUISA

Neste capítulo serão caracterizados e apresentados a metodologia de pesquisa utilizada neste trabalho, as etapas consideradas e sua descrição, a definição da unidade de pesquisa, o protocolo de pesquisa utilizado, coleta de dados e análise.

3.1 CARACTERIZAÇÃO DA PESQUISA

A presente pesquisa caracteriza-se pela sua natureza exploratória e descritiva, uma vez que foi realizada através de um estudo de caso em uma Instituição Financeira, identificando, analisando e relatando as atividades e procedimentos adotados para a implementação do SGSI baseado na Norma *BS*7799-2:2002.

A natureza exploratória é a estratégia de estudo de caso que é utilizada para explorar aquelas situações nas quais a intervenção que está sendo avaliada não apresenta um conjunto simples e claro de resultados. A natureza descritiva de um estudo de caso é a estratégia utilizada para descrever uma intervenção e o contexto na vida real em que ela ocorre (LIPSET; TROW; COLEMAN, 1956).

As estratégias de pesquisa de estudo de caso podem ser estabelecidas a partir de determinadas condições de sua realização. Yin (2003) estabelece três condições para o processo de escolha de uma estratégia de pesquisa: (a) tipo de questão de pesquisa proposta; (b) extensão de controle que o pesquisador tem sobre os eventos comportamentais ativos; e (c) maior enfoque em acontecimentos contemporâneos, em oposição a acontecimentos históricos.

A partir destas condições, Yin (2003) relaciona cada uma delas às principais estratégias de pesquisa nas ciências sociais – experimento, levantamento, análise de arquivos, pesquisa histórica e estudo de caso. Baseado nestas duas dimensões, foi estabelecido, pela *Cosmos Corporation*, o esquema apresentado no Quadro 5.

ESTRATÉGIA	Forma de questão de pesquisa	Exige controle sobre eventos	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

Quadro 5 – Situações relevantes para diferentes estratégias de pesquisa
Fonte: *Cosmos Corporation* (apud YIN, 2003).

Na presente pesquisa, as questões propostas evidenciaram a necessidade de acompanhamento do pesquisador durante o processo como um todo, ou seja, de seleção, de análise de componentes e elementos da Norma *ISO*/*IEC BS*7799-2, de modelagem de um SGSI e de sua implementação. O pesquisador participou do processo, porém não possuía controle sobre eventos comportamentais. Além disto, a pesquisa mostra a direção de seu foco em acontecimentos contemporâneos, ou seja, na necessidade da gestão da segurança da informação em um ambiente instável e altamente complexo sob o ponto de vista tecnológico, operacional e gerencial.

Desta forma, nesta pesquisa, optou-se pelo estudo de caso, haja vista tratar-se de uma investigação empírica que observou um fenômeno contemporâneo dentro do seu contexto da vida real, especialmente porque os limites entre o fenômeno e o contexto não estão claramente definidos (YIN, 2003).

3.2 DESENHO E ETAPAS DA PESQUISA

A pesquisa foi dividida em três etapas, conforme apresentado na Figura 4, a seguir: conceitual, prático-construtiva e conceitual.

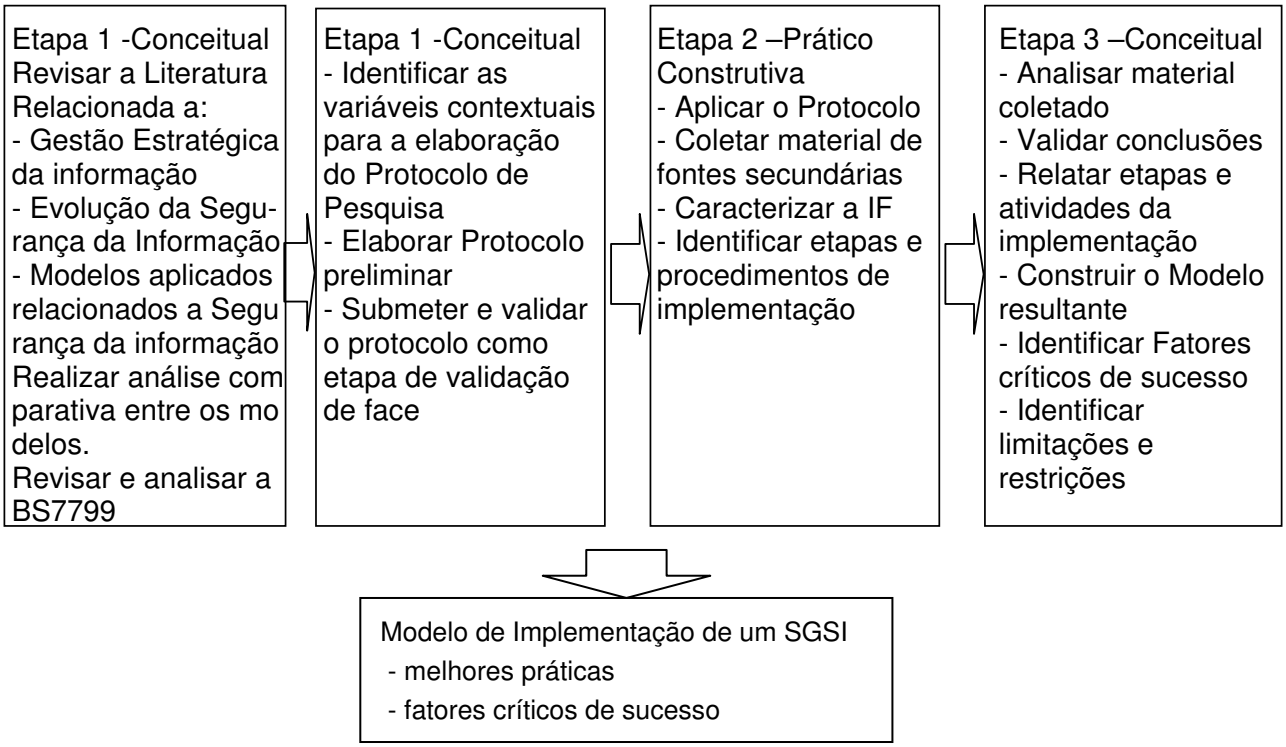

Figura 4 – Esquema do modelo de pesquisa

Fonte: o autor.

A primeira etapa, conceitual, foi constituída pelas seguintes atividades:

a) revisão da literatura disponível, relacionada à gestão estratégica da informação, e ao modo pelo qual o meio acadêmico tem abordado os principais temas e conceitos relacionados ao objeto da pesquisa;

b) revisão da literatura disponível, relacionada à segurança da informação e sua gestão, e ao modo pelo qual são abordados os principais temas e conceitos envolvidos;

c) identificação dos principais modelos aplicados à segurança da informação, bem como uma análise comparativa entre estes modelos;

d) revisão e análise dos componentes e elementos da Norma BS7799-2:2002;

e) identificação das variáveis contextuais consideradas no estudo de caso;

f) elaboração do protocolo preliminar de pesquisa, a ser utilizado durante a fase de validação de face;

g) análise do protocolo preliminar por um especialista na área de segurança da informação, para garantir a completeza e compreensão das variáveis do protocolo; e

h) aplicação do protocolo preliminar junto a um dos integrantes do projeto na IF, a título de validação de sua compreensibilidade.

Os dois últimos os procedimentos foram considerados como a validação de face do protocolo.

A segunda etapa, prático-construtiva, foi constituída pelas seguintes atividades:

a) aplicação do protocolo de pesquisa, obtido e já validado na primeira etapa, a dois diretores, a quatro gestores intermediários e a seis funcionários não-graduados, além de a dois consultores ligados ao projeto realizado na IF;
b) coleta dos materiais-fonte de informações secundárias;
c) caracterização e descrição da unidade de análise da pesquisa; e
d) identificação das etapas e procedimentos adotados no processo de implementação da Norma.

A terceira etapa, conceitual, foi constituída pelas seguintes atividades:

a) análise, pelo pesquisador, dos dados coletados, com base em procedimentos qualitativos de análise de conteúdo (fontes primárias e secundárias);
b) avaliação da consistência e validação das principais conclusões identificadas no item anterior, junto aos próprios entrevistados;
c) relato do estudo de caso (objeto da pesquisa), descrevendo as etapas e atividades adotadas e os fatores críticos de sucesso na implementação do SGSI, bem como outras observações relevantes para a compreensão do leitor em relação ao desenvolvimento do projeto; e
d) identificação das restrições e limitações, bem como das contribuições da pesquisa e de itens sugeridos para serem considerados em pesquisas futuras sobre o tema.

A adoção deste modelo de pesquisa resultará no modelo de implementação de um Sistema de Gestão de Segurança da Informação, bem como na identificação dos fatores críticos de sucesso desta implementação.

3.3 SELEÇÃO DA UNIDADE DE ANÁLISE

Nos estudos descritivos, uma clara definição da unidade de análise ajuda a delimitar o tema onde se quer aplicar uma pesquisa (DUBÉ; PARÉ, 2003). Na presente pesquisa, procurou-se identificar empresas com elevado grau de maturidade e sensibilidade para o tema da Segurança de Informação (FLEURY, 2003) e que atuasse em um segmento econômico relevante. Primeiramente, buscou-se identificar as empresas que fossem certificadas pela norma *ISO*/*IEC BS*7799-2. Constatou-se que, segundo o *ISMS International User Group* (Anexo F), em 2005 havia, no mundo, apenas 1.685 empresas certificadas, e apenas três destas estavam no Brasil.

No entanto, o fator mais relevante para a escolha da unidade de análise foi o fato de o pesquisador trabalhar em uma das empresas certificadas no Brasil e a única, dentre estas, que é pertencente ao mercado financeiro. O pesquisador fez parte da equipe do projeto de certificação, e isso lhe possibilitou, de maneira singular e inédita, amplo acesso às informações e documentos relativos ao mesmo. Haja vista a própria natureza do trabalho realizado – segurança da informação – o acesso a estes documentos seria totalmente impossibilitado a qualquer outro pesquisador, em função, inclusive, de restrições contratuais impostas através de termo de confidencialidade assinado pelos participantes do projeto. A unidade de pesquisa escolhida foi o Banco Matone S/A.

3.4 PROTOCOLO DE PESQUISA

O protocolo de pesquisa foi criado a partir dos principais componentes da Gestão de Segurança da Informação levantados na literatura e na norma *BS*7799-2:2002, contendo perguntas abertas. Foi aplicado na forma de entrevistas gravadas, conduzidas pelo próprio pesquisador ou registradas em papel, com dois Diretores, cinco Gestores, cinco colaboradores não-graduados e dois consultores envolvidos no processo de implementação do SGSI.

Para a definição das questões, foram utilizadas: o Quadro 6 referenciando os componentes e elementos utilizados para Gestão de Segurança da Informação.

Este protocolo foi validado pelo Sr. Fábio Ramos, profissional especialista da área de Segurança da Informação com as certificações CISSP, CISM e CIFI. A seguir, foi aplicado ao MSc. Carlos Alberto Carvalho, Diretor de Marketing do Banco Matone S/A e participante do projeto. O protocolo utilizado é apresentado a seguir.

PROTOCOLO DE PESQUISA

Respondente: _____

1) Comentar sobre a decisão estratégica da empresa em adotar a Norma *BS*7799 (Capítulo 0).

2) Comentar sobre o escopo adotado: Gerenciamento da Segurança da Informação para a Prestação de Serviços para Crédito de Pessoa Física na Matriz e Lojas Credimatone (Capítulo 1).

3) Comentar os termos: Integridade, Disponibilidade e Confidencialidade (Capítulo 3).

4) Comentar sobre o Sistema de Gestão da Segurança da Informação (SGSI) implantado, em relação às atividades do negócio e riscos da organização (Capítulo 4).

5) Comentar sobre a responsabilidade e o comprometimento da Alta Administração no SGSI, quanto ao estabelecimento das políticas de segurança, papéis e responsabilidades, comunicação da importância e dos objetivos, provimento dos recursos necessários, definição do nível de risco aceitável e condução de análises críticas (Capítulo 5).

6) Comentar sobre a revisão do SGSI, planejada pela Alta Administração, através da análise crítica de dados de auditorias internas e externas, dados históricos e oportunidades identificadas, modificação de procedimentos, provimento de recursos necessários (Capítulo 6).

7) Comentar sobre as melhorias do SGSI a partir dos conceitos de melhoria contínua, ações corretivas e preventivas (Capítulo 7).

8) Comentar os benefícios identificados com a adoção da Norma *BS*7799 e certificação do SGSI.

9) Comentar outros fatos relevantes a serem considerados.

Obrigado.

Quadro 6 – Protocolo de Pesquisa

Fonte: o autor.

3.5 COLETA DE DADOS

Os procedimentos de coleta de dados foram realizados através de fontes primárias e fontes secundárias.

A coleta de dados primários utilizou o protocolo de pesquisa apresentado no Quadro 6. As entrevistas foram realizadas conforme o Quadro 7.

RESPONDENTE	NÍVEL HIERÁRQUICO	OBSERVAÇÃO
Ernandi Ávila	Diretor Vice-Presidente	
Carlos Carvalho	Diretor de Marketing	Validação de Face
Cláudio Cappelletti	Gerente de Recuperação de Crédito	
Rosalva Rocha	Gerente de Contact Center	Não pertence mais ao quadro
Katia Magni	Gerente de Desenvolvimento de RH	Não pertence mais ao quadro
Fernanda Farias	Colaborador da Área de Recuperação	
Claudia Scherer	Colaboradora da Área de Contact Center	Trocou de Área de atuação
Sibele Schirmer	Colaboradora da Dir. Administrativa	
Rozane Silveira	Colaboradora da Área de RH	
André Palma	Consultor especialista em Segurança da Informação	Participou do Projeto
Gustavo Scotti	Consultor especialista em Segurança da Informação	Participou do Projeto

Quadro 7 – Relação dos respondentes do protocolo

Fonte: o autor.

A coleta dos dados secundários foi realizada através da análise dos documentos apresentados no Quadro 8.

DOCUMENTO	QUANTIDADE	FINALIDADE
Atas de Reunião de 2003	22	Reuniões do Comitê de Segurança, do Fórum de Segurança e do grupo de Multiplicadores
Atas de Reunião de 2004	16	Reuniões do Comitê de Segurança, do Fórum de Segurança e do grupo de Multiplicadores
Planos de Continuidade de Negócios	102	Planos de continuidade de negócios das diversas áreas e lojas, sistemas e recursos
Testes do Plano de Continuidade de Negócios	28	Relatório dos testes executados sobre o Plano de Continuidade de Negócios
Análise Crítica de Mudanças Técnicas	5	Relatório de avaliação de riscos na alteração de ambiente
Relatório de Monitoração de Capacidade	5	Relatório de acompanhamento de capacidade dos recursos computacionais
Relatórios de Ações Corretivas e Preventivas	92	Evidência das ações adotadas durante o projeto e sua manutenção
Macrocronograma de atividades	1	
Questionário de Avaliação de colaboradores	1	Avaliação de Treinamentos
Temas da Campanha de Segurança da Informação	1	
Escopo do *e-learning* para segurança da Informação	1	
Inventário de Ativos de Informação	10	
Responsabilidade sobre Documentos e aprovações	1	
Termos de Responsabilidade	8	Uso de Celulares, Modem, Computador Portátil
Diagramas de Topologia de Rede	2	
Análise de Risco	22	Registro de Análise de Risco, Plano de Tratamento de Risco e Declaração de
Listas de Presença de Treinamentos	141	Evidência dos treinamentos realizados
Listas de Presença de reunião de Multiplicadores	1	Evidência de reunião do grupo de Multiplicadores da segurança
Lista de Presença de Reunião de Gestores	1	Evidência de reunião de gestores
Registros de Incidentes	750	Apurar não-conformidades do sistema de gestão implantado
Contratos de Serviço	2	
Organograma	1	
Documentos de Constituição da IF	1	
Relatório da Auditoria Externa *DNV*	2	
Relatório de Analise de Vulnerabilidades	1	
Relatório de Análise Crítica do SGSI	1	
Relatório de Auditoria Interna	1	

Quadro 8 – Relação do material secundário

Fonte: elaborado pelo autor.

Por se tratar de implementação de uma norma de caráter fundamentalmente formalista e documentacional, o pesquisador obteve um grande número de documentos que, de forma detalhada, demonstraram como se desenvolveram as diversas etapas e atividades.

3.6 ANÁLISE DE DADOS

Para a análise dos dados coletados, foram utilizadas as técnicas de revisão interpretativa e construtiva, as quais, no decorrer do estudo de caso, permitiram identificar a construção evolutiva da implementação do SGSI na instituição financeira pesquisada.

A documentação primária coletada foi analisada de maneira sistemática e recursiva, buscando pontos de convergência que serviram como análise confirmatória dos elementos identificados na documentação secundária.

Os documentos secundários coletados foram documentos originados e aprovados pelos comitês de trabalho encarregados da condução do projeto. Inicialmente, os trabalhos foram conduzidos pelo comitê da Segurança da Informação. Em uma segunda etapa, este comitê foi dividido em dois outros: o primeiro, denominado de “Fórum de segurança da informação” e o segundo, de “Comitê gestor da segurança da informação”. Os membros dos respectivos comitês e sua sistemática são apresentados no decorrer deste relato. A aprovação formal da documentação, através dos citados comitês, garante a consistência e a validade dos resultados apresentados.

4 RELATO DO ESTUDO DE CASO

Neste capítulo será apresentados a empresa-objeto da pesquisa e um breve resumo de seu histórico. Serão apresentadas também as etapas envolvidas na implementação do SGSI, na primeira certificação, e na manutenção do sistema implantado. Também serão identificadas as principais decisões estratégicas adotadas.

4.1 A EMPRESA

A empresa-objeto da pesquisa, conforme foi anteriormente mencionado, é o Banco Matone S/A. O Banco Matone faz parte de um grupo de empresas que iniciou suas atividades em 1967, com a distribuidora de títulos Divalvest, sendo esta a primeira distribuidora de títulos autorizada pelo Banco Central a operar no Estado do Rio Grande do Sul. Alguns anos depois, a Divalvest trocou seu nome para Matone Distribuidora. O Banco Matone, principal empresa deste grupo, foi constituído em 1989, quando da transformação da Matone Distribuidora em banco múltiplo. É mercadologicamente caracterizado como um banco para clientes exclusivos (*private bank*). Na área de investimentos, sua diretriz está centrada no CDB Matone, para atender um segmento de clientes que valorizam atributos tais como rentabilidade diferenciada e atendimento totalmente personalizado. Em 1997, o Banco Matone iniciou sua atuação no segmento de crédito pessoal, com garantia de cheque através da constituição da rede de lojas Credimatone. Consideradas como a referência do mercado neste segmento, as 47 lojas do Credimatone foram vendidas para o HSBC em dezembro de 2004. A partir de 2005, as atividades estão focadas no crédito consignado em folha de pagamento para aposentados e pensionistas do INSS, funcionários públicos federais, estaduais e municipais, bem como para servidores das Forças Armadas. O crédito consignado é operado através de uma rede, de abrangência nacional, de mais de 450 correspondentes bancários e representantes. Em 2006, a previsão total de empréstimos é de 370 milhões de

reais, atingindo uma carteira de 1 bilhão de reais. Em junho de 2006, havia um total de 120 funcionários em todas as empresas.

4.2 EVOLUÇÃO DA SEGURANÇA DA INFORMAÇÃO NO BANCO MATONE

Neste item serão apresentadas, segundo a visão do autor, as duas etapas distintas e complementares que consolidaram a experiência de implementação do Sistema de Gestão da Segurança da Informação no Banco Matone, e a sua conseqüente certificação.

Na primeira etapa, serão apresentados os principais direcionadores que levaram a IF à preocupação com a Segurança da Informação, bem como as primeiras decisões e as atividades relativas à questão, realizadas entre agosto de 2001 e dezembro de 2002. Também serão apresentadas as preocupações que levaram a instituição a decidir-se pela busca da certificação *BS*7799-2:2002.

Na segunda etapa, será apresentado o quadro da situação do SGSI até aquele momento, os direcionadores envolvidos, as decisões estratégicas tomadas e as atividades realizadas até a conquista da certificação, no período de janeiro a agosto de 2003.

4.2.1 Primeira etapa – Diagnóstico e primeiros passos

Até meados dos anos 90, as principais mudanças do sistema financeiro brasileiro foram motivadas pela necessidade de administrar altas taxas de inflação. Até aquele momento, o progresso tecnológico alcançado, na área de TI, visava, basicamente, o aumento da velocidade de processamento.

No entanto, desde 1964, vinha se estabelecendo uma série de fundamentos jurídicos e legais, com o objetivo de direcionar os esforços para a administração dos riscos inerentes ao sistema financeiro. Destacam-se, entre estes diferentes aspectos legais, a Lei 4.595, de 31 de dezembro de 1964 (Lei da Reforma do Sistema Financeiro Nacional), que cria e regula o funcionamento do CMN, do BC e das IFs.

Através da Lei 6.024 de 13 de março de 1974 e do Decreto-Lei 2.321 de 25 de fevereiro de 1987, que definem a competência do BC para submeter as IFs a regimes de intervenção e liquidação extrajudicial (BRASIL, 2001), Lei 10.214 de 27 de março de 2001, que dispõe sobre a atuação das câmaras e dos prestadores de serviço de compensação e de liquidação, no âmbito do Sistema de Pagamentos Brasileiro e finalmente através da Resolução 2.882 de 30 de agosto de 2001, do CMN, que dispõe sobre o Sistema de Pagamentos Brasileiro e as câmaras e os prestadores de serviços de compensação e de liquidação que os integram.

Inseridas neste contexto, as IFs de pequeno e médio porte foram confrontadas com a necessidade de implantar níveis de serviço e de infra-estrutura tecnológica inéditos, uma vez que as exigências eram as mesmas, independentemente do porte da instituição, as quais exigiam vultosos investimentos, tanto em hardware e software, quanto na estruturação de novas áreas e na qualificação e capacitação de pessoal e, em particular, dos seus gestores.

Em face deste desafio, o Banco Matone estabeleceu sua primeira decisão estratégica fundamental: a da continuidade da atividade bancária e da realização dos investimentos necessários. Para evidenciar a relevância desta decisão, cabe salientar que, em 2001, o Estado do Rio Grande do Sul sediava oito Bancos – Banrisul, Banco Ficrisa-Axelrud, Banco Malcon, Banco John Deere, Banco Gerdau, Banco Renner e Banco Comercial do Uruguai e Banco Matone. O Banrisul era, e ainda é, o braço financeiro do Estado e uma instituição de grande porte. Por outro lado, os Bancos Gerdau, John Deere e Comercial do Uruguai faziam parte de conglomerados financeiros maiores, onde a atividade financeira era uma atividade complementar e tais investimentos poderiam ser financiados por suas controladoras. Restaram, desta forma, quatro Bancos de pequeno porte dependentes exclusivamente de sua atividade bancária. O Banco Malcon e o Banco Ficrisa-Axelrud definiram-se por retornar à condição de Financeira, deixando de atuar como Bancos. Posteriormente, em 2003, a Financeira Ficrisa-Axelrud foi adquirida e absorvida pelo Banco Matone S/A.

Desta forma, com o objetivo de atender aos requisitos do SPB, o Banco Matone, considerando que não possuía, em seu quadro de funcionários, pessoal capacitado e com experiência suficiente para desenvolver atividades desta natureza, iniciou, em março de 2001, a seleção de empresas de consultoria, na área de TI,

que pudessem realizar o diagnóstico do ambiente computacional existente e a identificação das atividades a serem realizadas.

Inicialmente, foram definidos alguns requisitos a serem considerados, baseados no histórico de contratações do Banco Matone: (a) a empresa selecionada deveria ser focada e especializada em soluções tecnológicas voltadas para processos; (b) deveria ser de porte pequeno ou médio, de maneira que o Banco representasse um cliente importante para a empresa; e (c) preferencialmente, deveria ser sediada no RS, de forma que esta proximidade possibilitasse em um maior nível de envolvimento e de comprometimento.

Durante a fase de prospecção e das primeiras abordagens, a primeira conclusão evidenciada foi de que o problema a ser enfrentado não era tecnológico, mas de segurança de informação. Desta forma, optou-se por restringir o universo pesquisado. As empresas pré-selecionadas que melhor atendiam às necessidades da IF foram: Axur Information Securit, E-Trust, Módulo e ISS. Foi feito um contato com a ISS, uma empresa de capital externo (o que era desfavorável). No entanto, esta não retornou o contato inicial. A Módulo possuía o maior porte entre as selecionadas, e era sediada no Estado do Rio de Janeiro; e as outras duas eram sediadas no Rio Grande do Sul e tinham uma boa experiência na área. As duas últimas empresas citadas foram convidadas, em separado, para a realização de diversas reuniões técnicas para detalhamento de escopo e definições comerciais. Esses encontros foram realizados ao longo de um período de 30 dias, e foram concluídos com a escolha da empresa Axur Information Securit para a realização do relatório diagnóstico intitulado: Relatório de Análise de Riscos e Vulnerabilidades do Banco Matone. O relatório foi gerado em 26 dias úteis e apresentado em agosto de 2001. Cabe salientar que na página 2 do dito relatório, estavam definidos, como objetivos estratégicos do Banco, os seguintes:

a) adequar a estrutura tecnológica do Banco Matone para atender aos requisitos do Sistema de Pagamentos Brasileiro;

b) reconhecer vulnerabilidades no ambiente do Banco Matone;

c) definir uma estratégia para correção dos problemas de segurança identificados;

d) classificar, por meio de uma análise de risco, as ameaças tecnológicas, humanas, naturais e físicas existentes no ambiente de negócio do Banco Matone.

Avaliando os itens relatados, se percebe importantes fundamentos, desde o inicio das preocupações: primeiramente, o de atender aos requisitos tecnológicos do SPB, do reconhecimento de que a IF possuía vulnerabilidades, da percepção de que segurança da informação está relacionada à análise de riscos e, finalmente, de que existem outros riscos, além dos tecnológicos, a serem considerados.

Neste diagnóstico trabalharam onze colaboradores da IF e oito consultores da empresa. Por parte da IF, havia um coordenador de projeto (no nível gerencial), um grupo executivo composto por um diretor e por três gerentes, e uma equipe técnica integrada por seis profissionais. Pelo lado da empresa contratada, havia um coordenador de projeto, um consultor de processos, um auditor e cinco técnicos especializados em segurança da informação.

No relatório diagnóstico apresentado, na página 6, no item B-Metodologia, observa-se que a consultoria utiliza, em seus serviços, metodologia própria, que se baseia nos padrões internacionalmente aceitos de segurança da informação do *British Standard* 7799 (*BS*7799) e do *Baseline Protection Manual*.

O relatório foi composto pelos seguintes itens: Sumário Executivo, Metodologia, Resultados Encontrados, Ameaças (Humanas, Físicas, Tecnológicas e Naturais) e Impactos (Administrativos, Financeiros, Imagem, Legais, Operacionais, Humanos), Análise de Ambiente Físico (Matriz e Filiais), Análise da Arquitetura de Rede, Análise das Estações de Trabalho, Análise de Servidores, Análise dos Equipamentos de Conectividade, Análise de Bancos de Dados, Análise de Sistemas Aplicativos, Análise de Processos Administrativos, Análise do Fluxo de Informações, Análise do Sistema de Controle de Acesso.

Foram identificadas as vulnerabilidades associadas e, para cada uma delas, foi detalhado o seguinte: nome da vulnerabilidade; breve descrição; análise do impacto da vulnerabilidade, em uma escala de 0 a 50, quanto aos aspectos humanos, operacional, legal e administrativo; análise da probabilidade de ocorrência da vulnerabilidade, em uma escala de 0 a 10; análise da vulnerabilidade, considerando os aspectos de confidencialidade, integridade e disponibilidade; cálculo do índice de criticidade, segundo metodologia própria; e, finalmente, recomendações a serem observadas. Abaixo, seguem alguns exemplos apresentados no relatório:

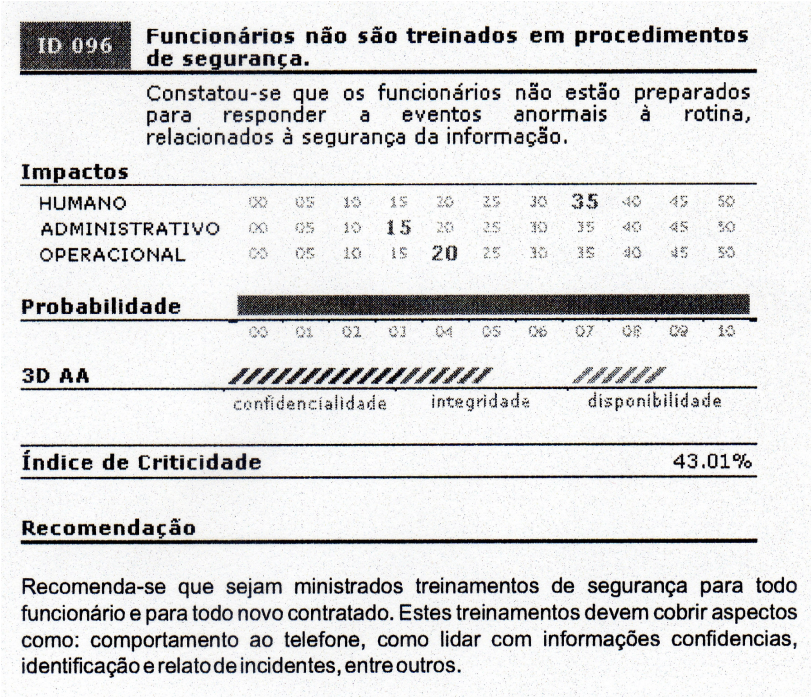

Figura 5 – Exemplo do diagrama de análise de vulnerabilidade

Fonte: Axur (2001).

É relevante salientar a descrição simples e objetiva das vulnerabilidades apresentadas, e as soluções igualmente simples a serem implementadas.

Com base na análise individual do índice de criticidade, para cada vulnerabilidade identificada, montou-se uma matriz de criticidade consolidando as vulnerabilidades, por capítulo, conforme o exemplo a seguir:

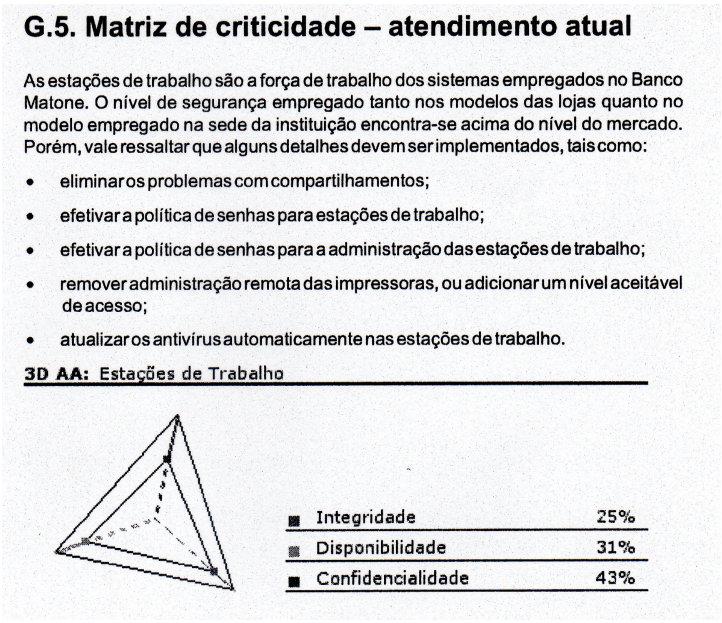

Figura 6 – Exemplo da matriz de criticidade

Fonte: Axur (2001).

Cabe destacar no dito relatório, na sua página 7:

O Banco Matone está passando por rápidas mudanças impulsionadas pelo crescimento vertiginoso de sua estrutura de lojas e da necessidade de suprir tecnologicamente as demandas crescentes. O que foi encontrado:

a) a rede interna do Banco Matone encontra-se com um nível inadequado de segurança para enfrentar as novas demandas (SPB);

b) os usuários não possuem treinamento em procedimentos de segurança da informação;

c) alguns colaboradores possuem privilégios inadequados sobre os processos, equipamentos e aplicações;

d) os processos, em sua maioria, não são documentados, e nem todos os colaboradores conhecem os seus procedimentos; e

e) a estrutura da rede está sendo subutilizada. Informações críticas são armazenadas nas estações de trabalho, sem rotina adequada de *backup*.

A partir da página 8 do relatório, cabe destacar o estudo comparativo (*benchmarking*) de maturidade em segurança da informação das instituições financeiras de médio porte em relação ao Banco Matone. As atividades relacionadas à segurança da informação, no Banco Matone foram classificadas em três níveis conforme exposto a seguir:

- abaixo do mercado: (a) não-utilização de certificados digitais para comunicação interna; (b) inexistência de *mail server*; (c) inexistência de sala segura para armazenamento de ativos críticos; d) procedimentos, em sua maioria, não documentados; (e) *backup* no próprio site; (f) inexistência de plano de gestão para segurança da informação; g) inexistência de *firewall*; (h) infra-estrutura de TI inapropriada; (i) utilização de senhas fracas; e (j) infra-estrutura de rede inadequada.
- média do mercado: (a) existência de política de segurança da informação; (b) possui softwares de gerência de processos de segurança; (c) inexistência de *Intrusion Detection System*; (d) *links* de dados gerenciados por terceiros; (e) não-conformidade na documentação de requerimentos técnicos; e (f) controle da mídia de *backups* é considerado inapropriado.

- acima do mercado: (a) comprometimento das gerências e dos executivos; (b) comprometimento dos colaboradores da área de TI; (c) configuração de hardware e de servidores; (d) segurança dos processos de informação das Lojas do Credimatone; e (e) agilidade na resolução de problemas.

Com base nos itens apresentados, ficou evidente que o Banco Matone, no final de 2001, estava bastante distante de uma situação que lhe possibilitasse tranqüilidade em relação à segurança da informação. O relatório foi analisado em profundidade e, com base neste diagnóstico, foi elaborado um plano de ação para minimizar as vulnerabilidades identificadas.

Para a execução deste plano de ação, observam-se algumas definições estratégicas relevantes, conforme exposto a seguir:

a) não seria constituída, na IF, uma área específica para a gestão de segurança da informação;

b) a responsabilidade sobre os aspectos relacionados à segurança da informação seria dos gestores intermediários; e

c) a segurança da informação seria gerida através de comitês.

A IF concluiu que o tema segurança da informação era muito importante para ser tratado por uma única área especializada e que o sucesso de sua implementação deveria ser objeto de preocupação de todos os gestores. A estrutura organizacional e a cultura da empresa favoreciam esta prática, uma vez que outros temas, tais como os do sigilo bancário e do desenvolvimento de recursos humanos já eram tratados da mesma forma descentralizada. No entanto, havia a preocupação em garantir a padronização de procedimentos. Então, optou-se por dar continuidade às atividades realizadas pela consultoria, que realizou o diagnóstico alterando seu perfil de atuação, de forma que atuasse como uma área de *Security Officer* terceirizada. A área de *Security Officer* é a área responsável por orientar as ações relacionadas à Segurança da Informação na empresa. Para legitimar e operacionalizar a execução do plano de ação, foram criados dois comitês: o de tecnologia e o administrativo. Ao Comitê de Tecnologia caberia a responsabilidade por todas as atividades técnicas de infra-estrutura tecnológica e de aplicações, tais como a implementação de *firewall*, a implementação de requisitos de segurança em

servidores e segurança de aplicativos. Ao Comitê Administrativo caberia a responsabilidade por todas as atividades extratecnológicas, tais como o treinamento de colaboradores, a revisão de sistemas, a criação ou adequação de procedimentos e padronização e a revisão de contratos e aspectos legais. O Comitê Tecnológico foi formado por analistas de sistemas, analistas de negócio, analistas de suporte e empresas terceirizadas, contratadas para atividades específicas. Este comitê foi coordenado pelo Gerente de TI. O Comitê Administrativo foi formado por colaboradores das áreas de RH, da assessoria jurídica, da tesouraria, da contabilidade e da área administrativa. Este comitê foi coordenado pelo Gerente Administrativo. O projeto, como um todo, ficou sob responsabilidade do Gerente de TI.

O plano de ação em questão foi executado entre os meses de outubro de 2001 e dezembro de 2002 e contemplou, em resumo, os seguintes aspectos:

a) elaboração e implementação do Plano Gestor de Segurança da Informação;

b) elaboração e implementação de sistemática de monitoração contínua do Plano Gestor;

c) elaboração e implementação de Política de Segurança da Informação para usuários e administradores;

d) elaboração e implementação de sistemática de monitoração contínua da Política de Segurança;

e) documentação do procedimentos das rotinas da área de Tecnologia da Informação;

f) análise de riscos e implementação de sistemática de segurança sobre Ativos de Segurança críticos;

g) implementação de sistemática de verificação contínua de vulnerabilidades, com ênfase na notificação de incidentes de segurança;

h) implementação de segurança de servidores;

i) implementação de *firewalls*; e

j) análise de vulnerabilidades no principal sistema aplicativo de geração de negócios.

Em 20/12/2002, foi realizada a última atividade deste plano de ação, que consistia de uma reunião para a prestação de contas das ações planejadas e

executadas, para o encerramento do projeto, e para a definição de novas etapas a serem realizadas, se fosse o caso. Participaram da reunião: Presidente, Vice-presidente, demais Diretores, Gerente Administrativo, Gerente de TI, Gerente de Contabilidade, Auditoria Interna, Consultoria para controles internos, participantes dos Comitês e consultoria contratada.

Nesta reunião, a IF chegou às seguintes conclusões:

a) os requisitos do SPB haviam sido atingidos, e o SPB foi implantado com sucesso, em 22/04/2002;

b) o sistema de gestão de segurança da informação havia sido implantado com sucesso;

c) os requisitos tecnológicos relacionados à segurança da informação haviam avançado muito e encontravam-se consolidados;

d) os requisitos administrativos e legais não haviam avançado na mesma proporção que os tecnológicos;

e) a decisão de descentralizar a ação da segurança da informação entre os gestores foi acertada;

f) a ação dos comitês, apesar de eficiente, não conseguia avançar quanto aos aspectos estratégicos;

g) não havia uma explicação razoável para a existência de itens que continuavam abaixo do padrão de mercado, após as diversas iniciativas e atividades realizadas; e

h) o modelo de implementação adotado havia sido eficiente, no entanto, havia esgotado suas capacidades.

Ainda durante a mesma reunião, foi estabelecido um intenso debate com o objetivo de identificar como a IF poderia avançar em relação à segurança da informação. Observou-se que, desde o inicio das atividades, ainda em 2001, sempre foi utilizado como fio condutor a *BS*7799-2:2002. Esta norma era o único padrão mundial que possibilitava a auditoria independente dos processos implantados e também, a partir desta auditoria, a certificação internacional das melhores práticas. Também foi observado que poucas empresas no mundo possuíam esta certificação, sendo somente duas destas no Brasil, e que nenhuma destas atuava na área financeira (Anexo F). Desta forma, ao final da reunião, conforme documentado em Ata, ficou definido o seguinte:

a) o Banco Matone desenvolveria um projeto para a conquista da primeira certificação da *BS*7799-2:2002 em uma instituição financeira das Américas, até o início do segundo semestre de 2003;

b) para a condução deste projeto, seria criado o Comitê de Segurança de Informações, em substituição aos antigos Comitês de TI e Administrativo. O Comitê mencionado seria formado pelos Diretores Presidente e Vice-presidente, demais Diretores e todos os gerentes de área; e

c) o escopo da certificação seria o processo de concessão de crédito nas Lojas do Credimatone em todo o Brasil e na Matriz do Banco Matone em Porto Alegre, Rio Grande do Sul.

É relevante destacar, nesta decisão estratégica, a objetividade, a dimensão, o foco e a clareza da meta a ser alcançada, inclusive quanto ao prazo definido.

Com base na documentação pesquisada e no relatório, (Anexo D), elaborado por Fabio Ramos (2004), serão apresentadas, a seguir e de maneira estruturada, os principais benefícios decorrentes desta decisão:

a) estabelecimento de um novo desafio, e com maior abrangência, a ser alcançada pela IF;

b) aumento da maturidade da empresa na condução de projetos (atividade relevante, haja vista a cultura da organização, em atuar orientada a projetos);

c) maior envolvimento e comprometimento das áreas administrativas;

d) conquista da certificação como uma conseqüência natural da implementação de um Sistema de Gerenciamento da Segurança da Informação bem implantado.

e) custo relativamente baixo da certificação, uma vez que grande parte das atividades de infra-estrutura tecnológica já estava implantada;

f) conquista da certificação como uma importante demonstração pública de que a IF possuía uma sistemática homologada de gerenciamento de riscos;

g) ganho institucional junto a órgãos reguladores (principalmente junto ao Banco Central) e parceiros de negócio (outras IFs); e

h) ganhos de imagem (visibilidade de marca) e de Marketing (junto aos clientes) pelo fato de ser uma IF certificada em segurança da Informação.

4.2.2 Segunda etapa – Conquista da certificação *BS7799-2:2002*

O relato desta segunda etapa foi baseado nos registros de reuniões realizadas pelos diversos Comitês e em depoimentos coletados, de maneira garantir a maior fidelidade possível quanto à cronologia e ao conteúdo das atividades realizadas.

No dia 13/01/2003, foi realizada a primeira reunião do Comitê de Segurança da Informação, para formular o planejamento do projeto de certificação. Este planejamento foi estruturado de maneira aderente aos requisitos do *PDCA* (*Plan-Do-Check-Act*), conforme estabelece a norma *BS*7799, e às características da cultura organizacional da IF.

Nesta reunião, ficou definido que o Sr. Daniel Matone, Diretor de Captação, seria o Líder do projeto e foi estabelecido o cronograma inicial das atividades a serem realizadas. Também ficou definido que a consultoria Axur seria a empresa de consultoria externa responsável pela condução do projeto. Também houve a leitura da Política de Segurança que era adotada na época, sua revisão e aprovação do novo conteúdo.

Cabe salientar alguns aspectos relevantes desta primeira reunião, que serão analisados abaixo:

a) a definição do Sr. Daniel Matone como líder do projeto implicava alguns aspectos favoráveis, tais como:

a.1) sinalização clara para toda a organização quanto ao comprometimento da Alta Administração com o projeto; e

a.2) os aspectos administrativos, que na primeira fase da implementação do SGSI haviam sido menos observados, passariam a ser priorizados, considerando que o líder deste projeto não era oriundo da área de TI.

b) a revisão e aprovação da Política de Segurança, já na primeira reunião, sinalizava uma condução objetiva, orientada para os resultados a serem alcançados e a determinação de manter todas as iniciativas positivas que já haviam sido desenvolvidas até então.

Em 20/01/2003, foi realizada a análise da efetividade da política de segurança adotada, e também foi definida a divulgação da política através de treinamentos a

serem realizados para todos os funcionários e da posterior verificação de adesão dos funcionários aos conceitos de segurança. Esta divulgação seria iniciada a partir de 30/01/2003, através de uma reunião de início formal do projeto (*project kick-off meeting*).

Em 22/01/2003, o Comitê propôs a criação de materiais de apoio e reforço à divulgação da Política. O Diretor de Marketing apresentou e ficou responsável pela confecção de *mousepad*, cartazes e proteção de tela com o tema da segurança da informação, bem como apresentou a estratégia que seria adotada na divulgação através da Intranet e *e-mails*. Apresentou, na mesma ocasião, o personagem "Segurinho", que foi prontamente aprovado.

As Figuras 7 a 9b apresentam alguns dos materiais produzidos.

Figura 7 – *Mousepad* da campanha
Fonte: Banco Matone (2003).

Figura 8 – Proteção de tela

Fonte: Banco Matone (2003).

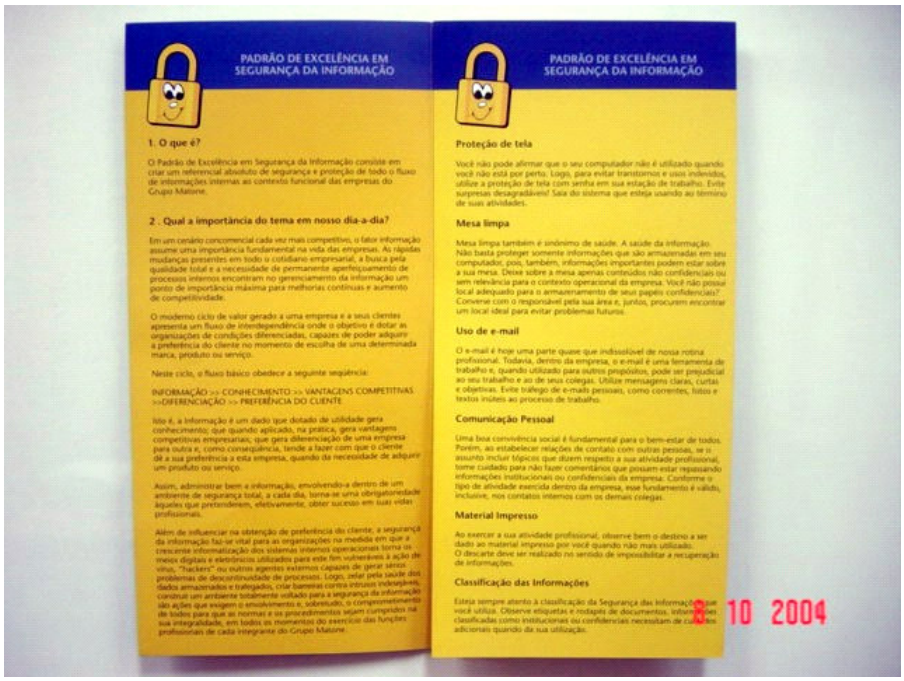

Figura 9a – Folder explicativo de conceitos de Segurança

Fonte: Banco Matone (2003).

Figura 9b – Detalhe do folder explicativo

Fonte: Banco Matone (2003).

Em 24/01/2003, foi lido e revisado o plano de continuidade de negócios do Banco Matone, implantado na etapa anterior. Tendo em vista sua complexidade e abrangência, a gerência de TI ficou responsável por dar continuidade a esta atividade.

Observa-se que o mês de janeiro de 2003 foi muito intenso em relação às atividades realizadas e às decisões tomadas. Após cada reunião do Comitê, grupos menores de trabalho realizavam reuniões paralelas para viabilizar ações a serem implantadas.

Em 31/01/2003, foi realizada a reunião de início formal do projeto, com o objetivo de notificar todo o quadro de pessoal da empresa sobre o projeto a ser desenvolvido, os envolvidos, patrocinadores, os papéis e responsabilidades de cada um, etapas do projeto e cronograma básico. No mesmo dia, foi iniciada uma intensiva etapa de treinamentos, em turmas de aproximadamente quinze funcionários, em quatro horários diários, com duração aproximada de uma hora cada, com o objetivo de repassar os principais conceitos de segurança. Todos os funcionários deveriam participar obrigatoriamente destes treinamentos (desde o presidente até os colaboradores nos níveis hierárquicos mais inferiores). Para atingir este objetivo, os conteúdos foram ligeiramente adaptados para cada público

específico, segundo suas atribuições e responsabilidades. Foi criada, por exemplo, uma turma exclusiva para o pessoal de portaria, outra para faxineiras, outra para diretores e presidente, e assim por diante. Inicialmente, os treinamentos foram ministrados pelos especialistas da consultoria externa, mas conforme as atividades foram avançando, muitos dos funcionários se destacaram e passaram a ministrar os conteúdos. O treinamento inicial foi composto pelos seguintes conteúdos: (a) definição de segurança da informação (inclusive confidencialidade, integridade e disponibilidade); (b) conhecimento e aceite da política de segurança da informação; (c) relevância da preocupação com a segurança da informação; (d) responsabilidades sobre a segurança da informação; (e) uso aceitável dos ativos de informação (contemplando correio eletrônico, estações de trabalho e programas de computador, sistemas telefônicos e celulares, equipamentos portáteis – *PDA*, *notebooks* e assemelhados); (f) controle de acesso físico; (g) responsabilidade sobre a movimentação, solicitação e troca de equipamentos e de software, bem como sobre o controle de software; (h) monitoração dos sistemas; (i) política de acesso – *login*, senhas, privilégios e manutenção de usuários; (j) política de "mesa limpa, tela limpa e descarte de informações"; (k) *backups*, ou cópias de segurança; (l) direito de propriedade intelectual e atendimento à legislação; (m) privacidade de dados e informações; (n) comunicação de incidentes de segurança; e (o) classificação e rótulo de informações – pública, restrita, institucional e confidencial.

Neste ponto, cabe fazer um parêntese e destacar que, logo no início dos treinamentos, foi observada a necessidade de criar um novo grupo de trabalho, com o objetivo de viabilizar a verificação de conhecimentos juntos aos funcionários. Foi criado, então, o Comitê de Multiplicadores da Segurança, composto inicialmente por doze por funcionários não-graduados, locados nas diversas áreas da empresa, mais identificados e com maior conhecimento sobre a temática da segurança da informação. A principal iniciativa do Grupo de Multiplicadores foi a criação da Campanha "Todo Dia é Dia de Segurança", cuja sistemática era a seguinte:

a) a cada semana, era definido um tema relevante sobre segurança da informação. Por exemplo, a "Semana da Privacidade de Dados" (citada na letra m do item anterior);

b) foram produzidos cartazes e materiais promocionais, e distribuídos entre as diversas áreas e ambientes (ver figuras abaixo);

c) os especialistas da consultoria elaboraram diversas questões a serem discutidas sobre o tema da semana;

d) nas sextas-feiras, um funcionário de cada área era escolhido, de forma aleatória, para responder o questionário, e, com base em suas respostas, toda a sua área era classificada;

e) as classificações possíveis eram: vermelho – com os dizeres “Atenção: você está em falta com a segurança da informação”; amarelo – com os dizeres “você ainda pode fazer mais pela segurança da informação”; e verde – com os dizeres “parabéns, continue assim”.

f) um cartaz (*banner)* com a classificação da área ficava exposto, durante toda a semana, na respectiva área;

g) uma lista, em ordem de classificação (*ranking*) das áreas, era publicada na Intranet;

h) a cada semana, um novo tema era selecionado, e novas questões eram incorporadas aos conteúdos da semana anterior.

Após a primeira semana, estabeleceu-se uma saudável, mas bastante competitiva, disputa entre as áreas. De imediato, os funcionários das áreas solicitaram a troca dos dias de aplicação dos questionários para a segunda-feira, com o objetivo de terem mais tempo para sua preparação. Era comum observar integrantes das diversas áreas “estudando” os temas, durante o intervalo do meio-dia.

Nas Figuras 10 a 12 estão demonstrados alguns exemplos dos materiais gerados para a Campanha:

Figura 10 – Cartaz da campanha de segurança

Fonte: Banco Matone (2003).

Figura 11a – *Banner* vermelho da campanha

Fonte: Banco Matone (2003).

Figura 11b – *Banner* amarelo da campanha

Fonte: Banco Matone (2003).

Figura 11c – *Banner* verde da campanha

Fonte: Banco Matone (2003).

Figura 12 – Foto do ambiente do *Call Center* com o *banner* verde
Fonte: Banco Matone (2003).

Mensalmente, baseado nas respostas coletadas pelo grupo de Multiplicadores, novas turmas de treinamento eram montadas, para reforço dos conteúdos que haviam sido avaliados como não estando bem sedimentados. De março a maio de 2003, foram realizados mais de 140 treinamentos, com uma média de aproximadamente quatro treinamentos por funcionário, tanto na Matriz do Banco quanto nas Lojas.

Cabe destacar que estes dois mecanismos (sistemática de treinamentos e campanha), relativamente simples, foram os principais responsáveis pela sinergia, comprometimento e mobilização necessários para o grande número de atividades realizadas.

Em 10/02/2003, foram definidas as áreas prioritárias para adequação do ambiente à Política de Segurança e foi iniciada a seleção dos controles a serem implantados, como por exemplo:

a) foi definido que o controle de acesso físico ao Banco não seria automatizado e que o mesmo seria realizado através da adequação dos crachás, que seriam de cores distintas para cada tipo de atividade;

b) foi revisada e aprovada a nova descrição de cargos, com a incorporação das responsabilidades de segurança de acordo com cada cargo;

c) foi aprovada a adoção de picotadoras de papel para descarte de documentos confidenciais; e

d) foi definida a melhoria da sala segura para ativos de TI, com a instalação de detectores de fumaça e grades adicionais de proteção.

Através desta sistemática, foram gradativamente realizadas e aprovadas todas as atividades previstas no planejamento do projeto. Alterações e adequações de processos, aspectos legais e outras necessidades foram sendo realizadas de maneira objetiva e rápida, aproveitando a mobilização e a característica da cultura organizacional da IF.

Paralelamente a estas atividades, foi escolhida a empresa *DNV – Det Norske Veritas* para a realização da auditoria externa. A auditoria externa foi planejada para ser realizada conforme as etapas a seguir: (a) pré-auditoria, a ser realizada durante três dias, com o objetivo de fazer a verificação da documentação gerada e sua conformidade com a norma *BS*7799-2:2002; (b) relatório da pré-auditoria, considerando as Não-conformidades e Observações[6] identificadas, a ser apresentado ao final desta pré-auditoria; (c) adequação do sistema, com o objetivo de eliminar as Não-conformidades e Observações – a ser feita em um prazo de 60 a 90 dias, negociado entre as partes; (d) auditoria propriamente dita, a ser realizada durante um período de sete dias úteis, considerando as atividades realizadas pelos colaboradores e sua adequação aos procedimentos documentados; e (e) recomendação ou não para a certificação – a ser apresentada ao final da auditoria.

De 23 a 25/04/2003, o Banco Matone recebeu o auditor-líder Mr. Birger Berggren (natural da Noruega) e, também compondo a equipe, o auditor brasileiro Fábio Pizzole, que atua em Caxias do Sul – RS, ambos integrantes da *DNV,* para a realização da pré-auditoria. À equipe de projeto foi incorporado um tradutor inglês-português (com bons conhecimentos em informática), para facilitar a comunicação direta entre o auditor-líder e os demais colaboradores. Ao final da pré-auditoria, foram identificadas duas Não-conformidades e cinco Observações. As duas Não-

[6] Não-Conformidade e Observação: São conceitos originários dos sistemas de gestão da qualidade e fazem parte do Relatório da Auditoria. Enquanto as Não-conformidades são falhas graves, que inviabilizam a Auditoria se não forem solucionadas, as Observações não representam maior gravidade. No entanto, elas devem ser consideradas como uma oportunidade para a realização de melhorias no sistema implantado (nota do autor).

conformidades deveriam ser solucionadas em um prazo de 60 dias, sob pena de impedirem a realização da auditoria externa. Estas duas Não-conformidades apresentadas foram: (a) o Plano de Continuidade de Negócios não contemplava a perda total da estrutura física; e (b) o método de análise de risco não considerava os ativos de segurança como base para a análise de risco. Com base nas Não-conformidades e Observações apresentadas, foram elaborados novos planos de trabalho, os quais foram iniciados, de imediato, pelas equipes envolvidas.

Cabe destacar uma iniciativa, que gerou grande transtorno durante a realização da pré-auditoria, que foi a contratação de um tradutor com conhecimentos em informática. O objetivo da contratação do tradutor era garantir que o depoimento dos colaboradores fosse espontâneo, sem a intervenção dos participantes do projeto. No entanto, o tradutor, com a intenção de "facilitar" o trabalho do auditor-líder, passou a "interpretar" o que os colaboradores estavam tentando dizer, o que prontamente era contestado pela equipe interna (que possuía proficiência na língua inglesa) que acompanhava o auditor. Apesar de possuir conhecimentos específicos em informática, este profissional possuía praticamente nenhum conhecimento em segurança da informação, e, desta forma, todo o trabalho de treinamento, educação e conscientização estava sendo prejudicado por esta "ajuda". Ao auditor norueguês, que nunca havia estado no Brasil, ficava a impressão de que a empresa não estava preparada, que os colaboradores não se faziam entender e que havia confusão no sistema implantado. Ao final do primeiro dia da pré-auditoria, foi realizada uma rápida reunião de avaliação, onde foi concluído que este tradutor deveria ser substituído de imediato. Na manhã seguinte, já estava compondo a equipe uma tradutora, com formação em música e praticamente nenhum conhecimento em informática, o que deu uma dinâmica totalmente nova e adequada à pré-auditoria.

Em 02/05/2003, haja vista o volume das atividades realizadas e o seu paralelismo, e também para atender aos requisitos da norma, houve uma reestruturação dos Comitês do projeto. Foi criado o Fórum de Segurança da Informação, composto pelos Srs. Alberto Matone – presidente, Ernandi Ávila – vice-presidente, Daniel Matone – Diretor de Captação e Líder do projeto, e também por um representante da consultoria, com o objetivo de avaliar e aprovar as decisões de nível estratégico. Foi criado, na mesma ocasião, o Comitê Gestor de Segurança de Informação, composto pelos antigos participantes do Comitê de Segurança da Informação e também por outros gerentes que não estavam formalizados como

participantes deste comitê, tais como o Gerente de Telemarketing e o Gerente da rede de Lojas. Este comitê tinha como objetivos definir e aprovar as decisões de níveis operacional e tático. O Líder do projeto e o representante da consultoria tinham assento nos dois comitês, e serviam como elo de ligação entre os mesmos. Esta providência deu novo impulso e dinâmica às decisões e acelerou o andamento das atividades que, em geral, passaram a ser solucionadas na própria reunião. As reuniões do Comitê Gestor aconteciam com maior freqüência e não dependiam da disponibilidade de tempo da Alta Administração.

Entre as primeiras atividades, iniciadas em janeiro, e aquele momento, já haviam sido gerados, aprovados e estavam disponíveis alguns documentos de formalização. tais como a IS 411.1 – Gestão do Fórum de Segurança de Informação, que estabelecia as responsabilidades e o funcionamento do Fórum, ou a IS 412.1 – Comitê Gestor de Segurança da Informação e a IS 415.1 – *Security Officer*, com finalidades análogas, relativas às responsabilidades e forma de atuação. Também ficou definido que toda a documentação pertinente à Segurança da Informação não poderia ser impressa, porém estaria disponível em área pública da Intranet. Esta providência minimizaria o problema de revisões e atualizações constantes de documentação, bem como o uso de formulários desatualizados, pois isto seria fundamental para garantir uma versão única e atualizada de toda a documentação que estava sendo gerada. Em geral, cada documentação visava atender a um objetivo ou controle específico, e continha, em média, de quatro a seis páginas, chegando a um total de 170 documentos. Uma solução engenhosa foi adotada para a publicação da documentação na Intranet, que está descrita através das etapas seqüenciais abaixo:

a) toda documentação gerada possuía uma única versão e era armazenada em uma única biblioteca na Intranet;

b) uma página referente à Segurança da Informação foi disponibilizada para acesso público de todos os funcionários;

c) nesta página, havia *links* para todas as áreas da empresa. Por exemplo, um funcionário da TI poderia “clicar” na área da TI;

d) dentro da área selecionada, havia *links* para todos os cargos disponíveis nesta área, como por exemplo, os de Analista de Sistemas ou de Analista de Suporte;

e) na lista de *links* relacionados ao cargo, havia *links* para todos os documentos pertinentes a este cargo; e

f) os *links* de documentos comuns a diferentes cargos, por exemplo, CS 511.1 – Política de Segurança de Informação, se repetiam nos diversos cargos, mas o documento sempre era único e estava atualizado.

Esta solução possibilitava que cada funcionário pudesse conhecer e estudar em profundidade todos os documentos relevantes e pertinentes ao seu cargo, sem a necessidade de efetuar pesquisas na biblioteca para localizar a documentação de seu interesse.

Em 06/05/2003 e 08/05/2003, foi aprovada, pelo Fórum de Segurança, a Análise de Risco de Ativos de Segurança. Como conseqüência disto, também foram aprovados o Plano de Tratamento de Riscos, o do Nível de Aceitação de Risco e a Declaração de Aplicabilidade.

Estes documentos compõem o núcleo do Sistema de Segurança da Informação e são resumidamente apresentados a seguir:

a) a Análise de Riscos identifica todos os ativos de Segurança envolvidos no processo a ser certificado. Ativos de Segurança são todos os equipamentos, pessoas, sistemas, processos, contratos ou bases legais relacionados, desde servidores e impressoras até o uso do crachá ou do telefone;

b) a Análise de Riscos estabelece, em seqüência, a probabilidade e o impacto de ocorrência de incidentes nestes ativos, considerando as suas disponibilidade, confidencialidade e integridade;

c) estabelece-se o Nível de Aceitação de Risco, que serve como uma “régua de corte”, sendo que deverão ser assumidos os ativos com risco abaixo do nível aceitável, e aqueles ativos com risco acima deste nível deverão ser tratados;

d) todos os ativos acima do nível de aceitação deverão ser objeto da Declaração de Aplicabilidade, que é um documento no qual será definido, para cada ativo em risco, qual controle é aplicável ou qual a justificativa para a sua não-aplicação; e

e) para os controles aplicáveis, deve ser definido qual será o Tratamento de Risco a ser adotado.

A adoção desta sistemática, através de um mecanismo de *PDCA* (melhoria contínua), é, em resumo, o que a auditoria externa avalia para recomendar a certificação.

Os níveis de aceitação foram formalizados nos documentos IS 40.1 – Análise e Tratamento de Riscos e RS 40.1.2 – Registro de Análise de Riscos, conforme exposto a seguir: a) risco (impacto *versus* probabilidade) com nível abaixo de 4 – risco aceitável, não requer controles; b) riscos acima de 4 até 6 – aplicação de controle recomendada, mas sujeita a avaliação; e c) riscos acima de 6 – controle obrigatório. Baseados nestas premissas, foram gerados os documentos RS 40.1.3 – Plano de Tratamento de Riscos e RS 40.1.4 – Declaração de Aplicabilidade.

Em 12/05/2003, foram aprovados, no seu formato final, os seguintes documentos:

a) GS 40 – Sistema de Gestão da Segurança da Informação;
b) IS 40.1 – Tratamento de Riscos;
c) IS 40.2 – Documentação do SGSI;
d) GS 50 – Responsabilidade da Alta Administração;
e) GS 60 – Revisão do SGSI pela Alta Administração;
f) IS 60.1 – Auditoria do SGSI; e
g) GS 70 – Melhora do SGSI.

Estes documentos descrevem todos os processos necessários à Gestão do Sistema de Segurança da Informação, para o estabelecimento do seu escopo definido.

Em 01/06/2003, foi realizada a primeira avaliação crítica da política de segurança da informação que havia sido implantada em 01/01/2003, frente às necessidades do negócio. Foi concluído que a mesma continuava efetiva. Também foram analisados os resultados da primeira auditoria interna, análise esta baseada no documento IS 60.1, e que foi iniciada em 15/06/2003 e realizada na Matriz e em cinco das lojas. Os resultados obtidos foram os seguintes: (a) os processos estão adequados às necessidades, porém é necessário um maior treinamento junto aos funcionários das lojas; (b) até o momento, a Matriz, em Porto Alegre, apresentou grande participação no processo, e a partir desta participação e interesse, foram realizadas muitas melhorias; (c) as áreas técnicas possuem conhecimento adequado dos procedimentos, mas não registram corretamente os procedimentos realizados; e

(d) foram registradas não-conformidades com relação ao descarte inadequado de informações nas lojas e também houve problemas de não-reporte de incidentes de segurança. Finalmente, foi definida a empresa *DNV* como a empresa que iria realizar a auditoria externa.

Os itens documentados pela auditoria interna geraram o 1º Relatório de Ações Corretivas e, em conseqüência, o 1º Plano de Melhoria de Revisão do SGSI. O plano de melhoria de revisão estabeleceu um redirecionamento das atividades de treinamento, no mesmo formato adotado anteriormente, priorizando as lojas e focando os seguintes conteúdos: (a) classificação e rotulação de informações; (b) descarte de informações; e (c) atividades a serem realizadas especificamente para a certificação e sobre como se daria o processo de auditoria externa.

Para incrementar e possibilitar o treinamento padronizado e eficiente de todas as 30 lojas, foi desenvolvido um programa de treinamento através de *e-learning*, utilizando a Intranet. O uso desta nova tecnologia e de uma formatação lúdica para o aprendizado foi um grande sucesso. O treinamento foi composto por 11 capítulos, e também foi elaborado um teste final, com questões aleatórias, onde o treinando deveria acertar no mínimo 70% delas. Um controle de tempo e freqüência de uso do *e-learning* possibilitou um efetivo acompanhamento da evolução do conhecimento sobre segurança da informação junto a todos os colaboradores da empresa. A Fiogura 13 apresenta uma das telas do *e-learning*:

Figura 13 – Exemplo do e-learning
Fonte: Banco Matone (2003).

Em 18/06/2003, foi realizada mais uma reunião do Fórum de Segurança, onde foram aprovados um cronograma complementar de treinamentos, ações de endomarketing e mais uma auditoria interna a ser realizada antes da auditoria externa.

Dentro da estratégia de endomarketing, foram produzidos novos materiais promocionais, tais como o selo promocional da *BS*7799 e a criação do boneco "Segurinho", representados nas Figuras 14 e 15.

Figura 14 – Selo institucional da segurança da informação
Fonte: Banco Matone (2003).

Figura 15 – Foto do Segurinho
Fonte: Banco Matone (2003).

Em 23/06/2003, foi recebido o cronograma elaborado pela *DNV*, referente às atividades a serem realizadas durante a auditoria externa, que seria executada entre os dias 26/06/2003 e 08/07/2003.

Pode-se afirmar que, nesta data, o SGSI estava implantado e o *PDCA* em pleno funcionamento. As reuniões do Fórum e do Comitê de Segurança estavam se realizando conforme os cronogramas definidos, e os incidentes estavam sendo "reportados" (ato de registrar em sistema próprio os incidentes de segurança identificados) e as melhorias identificadas estavam sendo implantadas. Uma certa ansiedade era percebida junto aos colaboradores, porém esta era resultado mais da expectativa referente à segunda visita do auditor externo do que em função das atividades que estavam sendo realizadas.

Em 26/06/2003, o auditor desembarcou no Rio de Janeiro e iniciou suas atividades, visitando as lojas daquela capital. Na manhã seguinte, ele foi a Brasília, e no terceiro dia, chegou a Porto Alegre. As principais atividades realizadas pelo auditor foram: (a) reunião formal de início de atividades; (b) revisão ou adequação do cronograma e das atividades a serem realizadas; (c) revisão do escopo a ser auditado e das alterações ocorridas na empresa deste a última visita; (d) verificação das não-conformidades e observações relatadas na última visita; (e) revisão da documentação, do Sistema de Gestão da Segurança da Informação e da política de segurança da informação; (f) avaliação da análise de risco – método, implementação e resultados; (g) revisão da declaração de aplicabilidade; e (h) revisão do plano de continuidade de negócios. Após esta revisão documentacional, as atividades de campo realizadas foram: (a) evidências de implementação de itens de controle de gerenciamento; (b) evidências referentes às pessoas (colaboradores); (c) evidências físicas e de ambiente; (d) evidências na área administrativa; (e) evidências na área de Marketing; (f) evidências de implementação de itens de controle de TI; (g) evidências de implementação de itens relevantes na área Legal; (h) evidências da organização para a segurança; e (i) visitas às lojas de Porto Alegre.

Segue a tradução do relatório final da auditoria, apresentado em 08/07/2003:

> Foram dois os focos desta primeira auditoria. O primeiro foi uma revisão completa da documentação e de sua atualização, tendo em vista as duas não-conformidades graves e as cinco observações relacionadas na pré-visita. O segundo foi auditar a implementação dos controles de segurança no processo-chave da companhia, em 5 lojas (do total de 30) e na matriz em Porto Alegre.
>
> O nível de segurança da informação do Banco Matone é alto. O Sistema de Gestão de Segurança da Informação implantado está coordenando as diferentes áreas da segurança, física, pessoal, administrativa e de TI. A plataforma de gerenciamento implantada é uma boa base para um aprimoramento futuro. Uma vez que o Banco Matone não é certificado pela *ISO*9000, também poderá aproveitar esta base.

> O método de análise de risco desenvolvido e a sistemática adotada poderão suportar a identificação de riscos em potencial. Em particular, a conexão entre risco, controle e procedimentos foi muito bem feita. Resta um número mínimo de riscos (acima do nível aceitável) a serem solucionados após uma contínua discussão no Fórum de Gestão da Segurança.
> Cinco lojas foram selecionadas (entre 30) para serem auditadas (Rio de Janeiro, Brasília, Canoas, São Leopoldo e Petrópolis (em Porto Alegre). Elas apresentaram muitas similaridades. Os controles de segurança são muito bons. De qualquer forma, pode ser aperfeiçoada a conscientização sobre o relacionamento entre os riscos identificados, as políticas de segurança e os controles atualmente implementados.
> O teste de conscientização, aplicado em 18 empregados entrevistados na matriz, foi bem sucedido. A conscientização por meio dos gestores e pessoal-chave poderia ser aumentada junto à comunidade, considerando o interesse nesta certificação.
> O desafio da segurança da informação é identificar que riscos são importantes e chegar a um consenso sobre como evitar um controle excessivo. Essa é a principal área para desenvolvimento futuro.
> Nossa conclusão é a de que o SGSI está operando satisfatoriamente, com um gerenciamento de infra-estrutura, ações corretivas, auditoria interna e gerenciamento de revisões.
> Data prevista para a próxima auditoria periódica: julho de 2004[7].

Após esta auditoria o Banco Matone S/A foi recomendado para a certificação *BS*7799-2:2002 e a mesma foi concedida em 27/10/2003.

[7] BERGGREN, Birgen. Relatório de auditoria interna, 2003. (tradução nossa)

5 MODELO RESULTANTE

Neste capitulo será apresentado um modelo geral do processo de implementação do SGSI, resultante desta pesquisa, e das etapas para implementação de um SGSI baseado na norma *BS*7799:2-2002. Como complemento ao modelo apresentado, também será apresentado um diagrama esquemático dos componentes implementados no SGSI e de sua relação com o que está estabelecido na norma *BS7799*-2:2002. Este item tem a finalidade de resumir para o leitor quais são os itens relevantes a serem observados na implementação de um SGSI. Finalizando o capítulo, será apresentada, segundo a visão do pesquisador, os fatores críticos de sucesso do sistema implementado.

5.1 ETAPAS DE IMPLEMENTAÇÃO

Uma importante observação a ser salientada é a constatação de que as práticas associadas à segurança da informação normalmente são iniciadas através de um projeto (com início e fim definidos), no entanto, as normas de gestão vigentes, tais como *ISO9001*, *ISO14001 e a própria BS7799-2:2002*, possuem incorporados em sua estrutura o conceito de melhoria contínua (conforme definido no item 0.2 – Abordagem, da BS7799-2:2002), o que, conseqüentemente, torna o sistema implantado (que é a conclusão do projeto), uma atividade de revisão cíclica permanente. Desta forma, a Segurança da Informação não é um objetivo, mas uma jornada (SCHMIDT, 2006). Não faz parte da presente proposta orientar quanto aos métodos a serem utilizados para o gerenciamento do projeto de implementação do SGSI. No entanto, o autor considera altamente recomendável a adoção de alguma prática consolidada para tal gerenciamento, de maneira que esta faça parte da infra-estrutura indispensável para a garantia de sucesso de implementação de um SGSI.

O modelo resultante de implementação do SGSI deste trabalho segue o modelo PDCA estabelecido por Deming (1990), quais sejam: Planejamento, Execução, Acompanhamento e Melhoria.

5.1.1 Planejamento

A primeira etapa, do Planejamento, deve ter por objetivo identificar os recursos (humanos, materiais, etc.), custos, prazos e atividades a serem realizadas para a condução do projeto de implementação do SGSI, bem como identificar as lacunas entre as atividades realizadas na organização e aquelas necessárias para a estruturação do SGSI conforme definido no capítulo 4 – Sistema de Gestão da Segurança da Informação, na norma BS7799-2:2002[8]. Esta etapa se encontra dividida em duas partes: Diagnóstico e Estratégia.

A primeira parte, de Diagnóstico, consiste na avaliação do grau de maturidade da organização em relação à segurança da informação, bem como na identificação dos ativos de segurança e vulnerabilidades associadas, conforme definido no item 4.2 – Estabelecendo e administrando o SGSI, da norma BS7799-2:2002, distribuindo-se na realização das seguintes atividades para IFs de pequeno porte:

a) definição do escopo do SGSI, da política do SGSI, da sistemática de avaliação de riscos;

b) identificação e classificação de todos os ativos de segurança e processos de negócio críticos para o SGSI;

c) realização da análise de ameaças (físicas, lógicas, humanas, etc.) associados aos ativos de segurança identificados;

d) realização da análise de vulnerabilidade para cada um dos ativos identificados; e

e) realização da análise e parametrização de riscos, para cada um dos ativos identificados, segundo a dimensão do impacto e o grau probabilidade de um incidente.

A conclusão da etapa de Diagnóstico deve apresentar como produto o documento Relatório de Análise de Risco.

---

[8] A sistemática adotada é aderente ao modelo conceitual definido pela International Federation of Accountants, no documento Managing Security of Information, citado no capitulo 2 – Fundamentação Teórica, item 2.1 – Gestão Estratégica da Informação.

A segunda parte, de Estratégia, visa identificar o grau de tolerância ao risco que a organização está disposta a enfrentar, bem como quais os controles de segurança a serem implantados na organização conforme definido no item 4.2 – Estabelecendo e administrando o SGSI, da norma BS7766-2:2002. As atividades realizadas são:

a) definição do grau de tolerância ao risco a ser aceito pela organização;

b) realização da avaliação de controles de segurança considerando a relação custo *versus* benefício;

c) definição das opções para o tratamento dos riscos e definição dos controles de segurança a serem implementados.

d) criação de um comitê de segurança com representação abrangente e executiva, e das demais estruturas organizacionais necessárias; e

e) definição da estratégia de implementação para o tratamento dos riscos e dos controles de segurança.

A conclusão da etapa da Estratégia deve apresentar como produtos os documentos Relatório de Declaração de Aplicabilidade e o Relatório de Plano de Ação.

5.1.2 Execução

A segunda etapa, de Execução, deve ter por objetivo a estruturação do SGSI, realizando as atividades previstas e implementando ações objetivas, tais como os controles de segurança selecionados. Esta etapa encontra-se dividida em duas partes: Tática e de Operação.

A primeira parte, da Tática, deve ter por objetivos a atribuição de responsabilidades, iniciar o plano de implementação e acompanhamento, implementar os processos de segurança definidos nas etapas anteriores e realizar os treinamentos necessários conforme previsto no item 4.2.1 – Implementação e operação do SGSI, da norma BS7799-2:2002. As atividades realizadas são:

a) criação da equipe de segurança da informação;

b) definição das regras e das responsabilidades relacionadas ao SGSI;

c) realização dos treinamentos operacional, tático e executivo, de forma sistemática; e

d) estabelecimento da conformidade técnica e legal dos processos de segurança.

A conclusão da etapa da Tática deve apresentar como produto a implementação da estrutura do SGSI.

A segunda parte, da Operação, visa implementar os processos operacionais a serem realizados a partir da estruturação realizada na etapa anterior, conforme definido no item 4.2.1 – Implementação e operação do SGSI da norma BS7799-2:2002, os quais possibilitarão a melhoria contínua e a consolidação do SGSI. As atividades realizadas são:

a) implementação dos controles definidos;

b) implementação das rotinas de segurança;

c) elaboração da redação final da documentação relacionada à segurança da informação;

d) implementação do processo de classificação da informação e controle de acesso; e

e) implementação da estrutura de resposta a incidentes.

A conclusão da etapa de Operação deve apresentar como produto o SGSI implementado e operacional.

5.1.3 Acompanhamento

A terceira etapa, de Acompanhamento, visa monitorar, ajustar, auditar e realizar a análise critica do SGSI implantado conforme definido no item 4.2.2 – Analisar criticamente e monitorar o SGSI, da norma BS7799-2:2002. As atividades realizadas são:

a) monitoração dos controles e das rotinas de segurança;

b) realização de auditoria dos processos e dos indicadores gerais de segurança;

c) garantia da consolidação da educação e da cultura de segurança da informação;
d) gerenciamento de eventos e incidentes de segurança; e
e) realização da análise crítica do SGSI.

A conclusão da etapa de Acompanhamento deve apresentar como produto o documento Relatório Periódico de Análise do SGSI.

5.1.4 Melhoria

A quarta etapa, de Melhoria, deve ter por objetivo gerenciar e implementar melhorias no SGSI conforme definido no item 4.2.3 – Manutenção e melhoria do SGSI, da norma BS7799-2:2002. As atividades realizadas são:

a) proposta de melhorias e validação dos novos processos do SGSI;
b) gerenciamento das mudanças do SGSI;
c) realização de ações preventivas e corretivas;
d) atualização da documentação correspondente; e
e) realização de ajustes dos processos de negócio, com base nas oportunidades de segurança identificadas.

O produto desta etapa é o documento de Plano de Ação de Melhorias.

5.2 COMPONENTES[9]

Neste item serão apresentados os componentes a serem implementados em uma IF de pequeno porte, a fim de estabelecer o SGSI. Também será estabelecida a conexão, de forma esquemática, entre os componentes identificados e três outros

[9] Componente: No contexto deste trabalho é um item ou ação definido na norma BS7799-2:2002 (item 2.4) a ser implementado no Sistema de Gestão de Segurança da Informação.

itens relevantes, quais sejam: um modelo conceitual, a norma BS7799-2:2002 e o modelo resultante. O modelo conceitual usado como referencial é o documento Managing Security of Information (MSI) apresentado no item 2.1 – Gestão Estratégica da Informação, do presente trabalho. Com relação a norma BS7799 o referencial utilizado é o que foi apresentado no item 2.4 - Norma BS7799-2:2002, também apresentado neste trabalho e com relação ao modelo resultante é utilizado como referencial o que foi apresentado no item 5.1 anterior. O Quadro 9 apresenta o diagrama esquemático:

COMPONENTE	ETAPA DO MODELO RESULTANTE	ATIVIDADE DO MSI	CAPÍTULO DA BS7799-2:2002
Definição do escopo e diretrizes do SGSI	Planejamento	Desenvolvimento de Políticas	4.1, 4.2 e 4.3
Análise de Risco dos Ativos de Segurança	Planejamento	Projeto	4.2
Declaração de Aplicabilidade	Planejamento	Projeto	4.2
Plano de Tratamento de Riscos	Planejamento	Projeto	4.2.1
Implantação da Estrutura, Rotinas e Controles de Segurança	Execução	Papéis e Responsabilidades; Execução	4.2.1
Treinamento e Conscientização	Execução	Consciência, treinamento e instrução; Execução	4.2.1
Sistemática de Resposta a Incidentes	Execução	Execução	4.2.1 e 7.1
Monitoração das Rotinas e Controles	Acompanhamento	Monitoração	4.2.2
Auditoria Interna	Acompanhamento	Monitoração	4.2.2 e 6.4
Análise Crítica do SGSI pela Alta Administração	Acompanhamento	Monitoração	4.2.2, 6.1, 6.2 e 6.3
Ações Corretivas, Preventivas e Plano de Melhoria	Melhoria	Monitoração	4.2.3, 6.3, 7.1, 7.2 e 7.3
Documentação	Execução e Melhoria	Execução	4.3
Responsabilidade da Alta Administração	Todas as Etapas	Desenvolvimento de Políticas	5.1 e 5.2
Revisão do SGSI pela Alta Administração	Melhoria	Monitoração	6.1 e 6.2

Quadro 9 – Diagrama esquemático de componentes implementados

Fonte: o autor.

5.3 FATORES CRÍTICOS DE SUCESSO

Esta seção apresenta os fatores críticos de sucesso, identificados no processo de implementação do Sistema de Gestão da Segurança da Informação na empresa estudada, de acordo com o relatado na Seção 4.2 do presente trabalho. Conforme apresentado na referida seção, a experiência do Banco Matone nesta implementação se deu em duas etapas complementares e contínuas. A primeira destas foi a de Diagnóstico e primeiros passos (ver Seção 4.2.1); e a segunda foi a da conquista da certificação (ver Seção 4.2.2).

Para a obtenção dos fatores críticos apresentados a seguir, inicialmente foram relacionados pelo autor, a partir da análise da documentação coletada e referências dos entrevistados, uma lista das decisões estratégicas, atitudes e ações relevantes que garantiram o sucesso da conclusão do projeto de implementação e a obtenção da certificação desejada.

Posteriormente esta lista foi confrontada com o referencial teórico para classificação da relevância de fatores críticos, segundo a proposição de Pinto e Sleven (1983 apud RABECHINI JR.; CARVALHO; LAURINDO, 2002) sobre o tema, que é categorizado conforme a seguir:

a) missão do projeto;
b) suporte gerencial;
c) planejamento;
d) cliente consultor;
e) administração de pessoal;
f) tarefas técnicas;
g) aceite do cliente;
h) monitoramento;
i) comunicação; e
j) gerência conciliadora.

Após essa categorização prévia, a lista foi revisada descartando-se os itens menos referidos e aqueles não categorizados. Junto a cada fator crítico identificado a seguir, está apresentada a sua correspondência com o referencial teórico.

Os fatores críticos relacionados aplicam-se exclusivamente ao estudo de caso em questão, para o ambiente e maturidade de gestão que a IF (que foi o objeto da presente pesquisa) apresentava no momento da condução do projeto, e não pode ser generalizado para outras instituições ou circunstâncias. Entretanto, a experiência prática relatada neste trabalho serve como um referencial para as lideranças que conduzirem um projeto de implementação de um Sistema de Gestão da Segurança da Informação em uma IF de pequeno porte. Na primeira fase de implementação – (Diagnóstico e primeiros passos) são destacados os seguintes fatores críticos de sucesso:

Fator Crítico de Sucesso Identificado	**Categoria do Referencial Teórico**
Definição pela continuidade da atividade bancária da IF	Missão do projeto
Garantia dos investimentos necessários para adequação ao SPB	Planejamento
Processo de seleção da empresa de consultoria na área de segurança e definição dos requisitos para fornecedores	Suporte Gerencial
Escopo do relatório diagnóstico e alinhamento com os objetivos estratégicos do Banco	Planejamento
Plano de ação para minimizar vulnerabilidades, baseado no relatório diagnóstico	Tarefa técnica
estrutura organizacional baseada em comitês: Comitê Administrativo e Comitê de TI	Administração de pessoal e monitoramento
Decisão de desenvolver o projeto de conquista da certificação em segurança da informação e definição objetiva do escopo, meta e data	Planejamento

Quadro 10 – Fatores Críticos de Sucesso x Referencial Teórico da primeira fase

Fonte: o autor.

Na segunda fase de implementação (Conquista da certificação) são destacados os seguintes fatores críticos de sucesso:

Fator Crítico de Sucesso Identificado	**Categoria do Referencial Teórico**
Sinalização clara, para toda a organização, do comprometimento da Alta Administração; e definição da liderança do projeto por um Diretor	Aceite do cliente e Gerência conciliadora
Priorização dos aspectos administrativos e liderança do projeto por um executivo que não pertencia à área de TI	Administração de pessoal, Tarefas técnicas e Monitoramento
Treinamentos curtos, continuados e para todos, sem distinção	Comunicação
Estrutura de projeto organizada através de comitês: Fórum de Segurança para as questões estratégicas; Comitê Gestor da Segurança para as ações táticas e técnicas; e Comitê de Multiplicadores da Segurança, para as questões operacionais e motivacionais	Administração de pessoal, Aceite do cliente, Comunicação
Iniciativas de mobilização, tais como a campanha “Todo dia é dia de Segurança”	Comunicação
Criação do personagem “Segurinho” e dos materiais de apoio, tais como mousepads, proteção de tela, folder explicativo, entre outros	Comunicação
Uso da intranet para arquivamento e apresentação da documentação pertinente, bem como restrição de impressão	Monitoramento, Comunicação
Uso do *e-learning* como ferramenta de treinamento para as lojas, e, na Matriz, para reforço deste aprendizado	Administração de pessoal e Comunicação

Quadro 11 – Fatores Críticos de Sucesso x Referencial Teórico da segunda fase

Fonte: o autor.

6 CONTRIBUIÇÕES E CONCLUSÕES

Este capítulo sintetiza os resultados do estudo de caso realizado. O objetivo principal desta pesquisa, de descrever o processo de implementação do Sistema de Gestão de Segurança da Informação em uma Instituição Financeira de pequeno porte, foi atingido através da identificação e consolidação de um modelo do processo de implementação de um SGSI, contemplando as etapas e as atividades a serem realizadas em cada etapa. Com isto, os objetivos específicos também foram alcançados, a partir da identificação dos componentes a serem estabelecidos em um SGSI e dos fatores críticos de sucesso apontados neste processo.

Desta forma, as questões de pesquisa também foram respondidas, a partir do modelo resultante deste trabalho, que estabelece como a segurança da informação pode ser melhorada e como implementar um SGSI em uma Instituição Financeira de pequeno porte, assim como quais os principais fatores críticos de sucesso desta implementação.

6.1 CONTRIBUIÇÕES TEÓRICAS

A presente pesquisa buscou contribuir com o meio acadêmico, evidenciando, através de um estudo aplicado, a importância e relevância da informação, a gestão estratégica da informação e os atributos da qualidade da informação, conforme demonstrado no capítulo 2 – Fundamentação Teórica (e, em especial, na Seção 2.1 – Gestão Estratégica da Informação). Como exemplo, pode ser citada a estruturação que McGee e Prusak (1994) sugerem, em ordem de importância, para o conjunto informacional:

a) informação na definição da estratégia, envolvendo informações atuais e precisas sobre o ambiente de mercado, as quais permitem identificar ameaças e oportunidades;

b) informação para a execução da estratégia, propiciando novas alternativas para a elaboração de processos que possam criar e oferecer produtos e serviços diferenciados; e

c) informação para retroalimentação, onde a empresa deve conseguir criar um ambiente de aprendizado constante e uma estrutura flexível, que facilmente consiga se adaptar aos objetivos definidos.

Com relação à qualidade da informação, foi citada a classificação de Strong, Lee e Wang (1997) em quatro dimensões – qualidade intrínseca, acesso aos dados, contextual e representatividade – com diferentes elementos dentro de cada uma destas dimensões.

Outra contribuição encontra-se na revisão histórica da evolução do tema da Segurança da Informação na área da TI (ver Seção 2.2 – Segurança da Informação no Âmbito da TI), suas implicações na sociedade e nas organizações, assim como a identificação dos principais modelos e práticas formalizados na área da Segurança da Informação, como o COBIT, ITIL, BS7799-2:2002, entre outras (ver Seção 2.3 – Modelos Aplicados). E, finalmente, através de uma comparação entre estes modelos aplicados de maior relevância na atualidade, buscou-se evidenciar a principal área de conhecimento e o foco das práticas de segurança de informação, conforme exposto na Seção 2.3.4 – Análise Comparativa.

6.2 CONTRIBUIÇÕES PRÁTICAS

Através de uma experiência prática, esta pesquisa contribui com um roteiro voltado para gestores e executivos de instituições financeiras de pequeno porte, bem como para profissionais ligados à gestão da segurança da informação, propondo um método sistematizado para a implementação de um SGSI.

O modelo resultante apresentado sugere os passos metodológicos necessários para a implementação do SGSI, baseados nas melhores práticas identificadas.

O diagrama esquemático do Quadro 9 traz um resumo dos principais componentes a serem observados pelos executivos de instituições financeiras de pequeno porte, quando da implementação do SGSI.

O presente estudo também serve como uma orientação estruturada para as organizações que já possuem um SGSI e que estejam buscando a certificação nesta área.

De modo complementar, espera-se que o mesmo possa servir de apoio para administradores preocupados em minimizar os riscos envolvidos nas atividades de gestão de segurança da informação e na condução de projetos de implementação, no Brasil, de normas internacionais.

6.3 LIMITAÇÕES DA PESQUISA

Esta pesquisa trata de um estudo de caso em uma única organização da área financeira e de pequeno porte, não possibilitando generalizar seus resultados.

O estudo de caso foi realizado com base no projeto de implementação do SGSI da referida IF realizado entre 2001 e 2003 a partir da análise documental e de depoimentos de participantes do projeto. O fato de o autor participar do grupo de trabalho que executou o projeto também pode ter acrescentado um viés às análises. No entanto, tanto quanto possível, procurou-se minimizar tal efeito, seja retornando os resultados para concordância dos demais integrantes da equipe do projeto, seja buscando suporte no referencial teórico de base.

6.4 PESQUISAS FUTURAS

Em função da abrangência, relevância e generalidade dos conceitos invocados, esta pesquisa poderá servir de base para estudos similares na área de Segurança da Informação, em outras Instituições Financeiras de porte semelhante à estudada ou em diferentes empresas atuantes em outras áreas de serviços (seguradoras, fundos de pensão, previdências privadas, etc.).

6.5 CONCLUSÕES

Os temas de Gestão da Informação e de Segurança da Informação têm sido estudados, há algum tempo. Porém, foi a partir de 2001 que estes temas adquiriram maior evidência. Os modelos publicados e aplicados contêm um conjunto de itens para a Gestão da Segurança da Informação, porém a maioria deles não provê, ou provê apenas fracamente, os passos metodológicos de como devem ser implementadas práticas de segurança da informação. Sendo assim, acredita-se que esta pesquisa possa servir como ponto de partida para novas iniciativas na área de gestão de segurança da informação, área esta ainda relativamente carente de estudos, haja vista o pequeno número de casos de empresas certificadas no Brasil.

REFERÊNCIAS

AXUR Information Security. Relatório de análise de risco e vulnerabilidades do Banco do Matone. Porto Alegre: Axur, 2001.

BACON, Francis. **Nova Atlântida**. 1627. Disponível em: <http://www.comciencia.br/reportagens/genoma/genoma6.htm>. Acesso em: 13 ago. 2005.

BANCO MATONE. **Site institucional**. 2003. Disponível em: <http://www.bancomatone.com.br>. Acesso em: 13 ago. 2005.

BRASIL. Banco Central do Brasil. **Sistema de pagamentos brasileiro**. 2002. Disponível em: <http://www.bcb.gov.br/?SPB>. Acesso em: 11 jul. 2005.

BRASIL. Circular nº. 3.057, de 31 de agosto de 2001. Aprova regulamento que disciplina o funcionamento dos sistemas operados pelas câmaras e pelos prestadores de serviços de compensação e de liquidação que integram o sistema de pagamentos. **Banco Central do Brasil**. Disponível em: <http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=101164388&C=&ASS=CIRCULAR+3.057>. Acesso em: 12 maio 2006.

BRASIL. Circular nº. 3.101, de 01 de abril de 2002. Regulamenta a conta Reservas Bancárias institui e regulamenta a Conta de Liquidação no Banco Central do Brasil. **Banco Central do Brasil**. Disponível em: <http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=102053443&C=&ASS=CIRCULAR+3.101>. Acesso em: 12 maio 2006.

BRASIL. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Fóruns do Planalto**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm>. Acesso em: 12 maio 2006.

BRASIL. Instrução CVM nº 358, de 03 de janeiro de 2002. Dispõe sobre a divulgação e uso de informações sobre ato ou fato relevante relativo às companhias abertas, disciplina a divulgação de informações na negociação de valores mobiliários e na aquisição de lote significativo de ações de emissão de companhia aberta, estabelece vedações e condições para a negociação de ações de companhia aberta na pendência de fato relevante não divulgado ao mercado, revoga a Instrução CVM

nº 31, de 8 de fevereiro de 1984, a Instrução CVM nº 69, de 8 de setembro de 1987, o art. 3° da Instrução CVM n° 229, de 16 de janeiro de 1995, o parágrafo único do art. 13 da Instrução CVM 202, de 6 de dezembro de 1993, e os arts. 3º a 11 da Instrução CVM nº 299, de 9 de fevereiro de 1999, e dá outras providências. **CVM – Comissão de Valores Mobiliários**. Disponível em: <http://www.cvm.gov.br/asp/cvmwww/atos/exiato.asp?File=%5Cinst%5Cinst358.htm>. Acesso em: 12 maio 2006.

BRASIL. Lei nº. 10.214, de 27 de março de 2001. Dispõe sobre a atuação das câmaras e dos prestadores de serviços de compensação e de liquidação, no âmbito do sistema de pagamentos brasileiro, e dá outras providências. **Dataprev**. Disponível em: <http://www010.dataprev.gov.br/sislex/paginas/42/2001/10214.htm>. Acesso em: 12 maio 2006.

BRASIL. Lei nº. 4.595, de 31 de março de 1964. Dispõe sobre a política e às instituições monetárias, bancárias e creditícias, cria o Conselho Monetário Nacional e dá outras providências. **Societário**. Disponível em: < http://www.societario.com.br/lei4595.html>. Acesso em: 12 maio 2006.

BRASIL. Lei nº. 6.024, de 13 de março de 1974. Dispõe sobre a intervenção e a liquidação extrajudicial de instituições financeiras, e dá outras providencias. **Banco Central do Brasil**. Disponível em: <www.bcb.gov.br/pre/leisedecretos/Port/lei6024.pdf>. Acesso em: 12 maio 2006.

BRASIL. Resolução nº. 2.554, de 29 de setembro de 1998. Dispõe sobre a implantação e implementação de sistema de controles internos. **Banco Central do Brasil**. Disponível em: <http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=098186548&C=2554&ASS=RESOLUCAO+2.554>. Acesso em: 12 maio 2006.

BRASIL. Resolução nº. 2.882, de 30 de agosto de 2001. Dispõe sobre o sistema de pagamentos e as câmaras e os prestadores de serviços de compensação e de liquidação que o integram. **Banco Central do Brasil**. Disponível em: <http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=101163546&C=&ASS=RESOLUCAO+2.882>. Acesso em: 12 maio 2006.

BRITISH Standards Institute. **Information security managemente systems**: specification with guidance for use: BS7799-2:2002. London: Editora BSI, 2002.

BRODBECK, A. F.; KALB, L. R.; BREI, V. Governança de TI: medindo o nível de serviços acordados entre as unidades usuárias e o departamento de sistemas de informação. In: ENCONTRO ANUAL DA ANPAD, 28., 2004, Curitiba, **Anais...** Curitiba: ANPAD, 2004. 1 CD-ROM.

COBB, S. **The mother of all security standard? Spectria infosec article**. 2001. Disponível em: <http://www.infosec.spectria.com/articles/art-bs7799.htm>. Acesso em: 14 maio 2005.

DEMING, W. E. **Qualidade**: a revolução da administração. Rio de Janeiro: Marques Saraiva, 1990.

DUBÉ, Line; PARÉ, Guy. Rigor in IS positivist case research: current practices, trends and recommendations. **MIS Quarterly**, Minneapoles, v. 27, n. 4, p. 597-601, Sept. 2003.

FARIAS JR., Ariosto. **Nova norma garante segurança da informação.** 2002. Disponível em: <http://www.serasa.com.br/serasalegal/05-fev-02_m2.htm>. Acesso em: 28 jul. 2005.

FLEURY, Elio Fontoura. **A proteção da informação**: a conscientização e o estágio de desenvolvimento apresentado por uma amostra de indústrias gaúchas frente à NBR ISO/IEC 17.799/2001. 2003. 116 f. Dissertação (Mestrado Profissional) – Programa de Pós-Graduação em Administração, Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2003.

GONÇALVES, M. **Firewalls**: guia completo. Rio de Janeiro: Ciência Moderna, 2000.

HEFFERAN, C. **BS7799 – Information security management**. 2000. Disponível em: <http://www.istc.org.uk/bs7799.html>. Acesso em: 24 maio 2005

HOUAISS, Antônio; VILLAR, Mauro de S. **Dicionário Houaiss da língua portuguesa**. 2001. Disponível em: <http://houaiss.uol.com.br/busca.jhtm>. Acesso em: 12 nov. 2005.

INTERNATIONAL STANDARD. **ISO** / **IEC 17799 – information technology - code of practice for information security management**. Genebra: International Standardization Organization, 2000.

ISACA. Serving IT Governance Professionals. **COBIT**. 2004. Disponível em: <http://www.isaca.org/>. Acesso em: 17 jul. 2005.

LIPSET, S. M.; TROW, M.; COLEMAN, J. **Union democracy**: the inside politics of

the International typographical union. New York: Free Press, 1956.

MCGEE, Jame; PRUSAK, Laurence. **Gerenciamento estratégico da informação:** aumente a competitividade e a eficiência de sua empresa utilizando a Informática como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

MÓDULO SECURITY. **BS7799-1**. 2001. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 17 jul. 2005.

MORAES, G. D.; TERENCE, A. C. F.; ESCRIVÂO FILHO, E. A tecnologia da Informação como suporte à gestão da informação na pequena empresa. **Revista de gestão da tecnologia e Sistemas de informação**, São Paulo, v. 1, n. 1. p. 28-44, set./dez. 2004.

PEIXOTO, Rodney de Casto. **Marcos divisórios na segurança da informação**. 2004. Disponível em: <http://www.issabrasil.org/artigos_0003.asp>. Acesso em: 12 jul. 2005.

PIPINO, Leo L.; LEE, Yang W.; WANG, Richard Y. Data quality assessment. **Communications of the ACM**, New York, v. 45, n. 4, p. 211-219, Apr. 2002.

RABECHINI JR, Roque; CARVALHO, Marly M. de; LAURINDO, Fernando J. B. Fatores críticos para implementação de gerenciamento por projetos: o caso de uma organização de pesquisa. **Revista Produção**, São Paulo, v. 12, n. 2, 2002. Disponível em: <http://www.vanzolini.org.br/revistaproducao/12_02_2002.htm>. Acesso em: 12 maio 2005.

RAMOS, Fábio F. **BS7799**: certificar ou não certificar? Eis a questão. 2004. Disponível em: <http://www.axur.com.br>. Acesso em: 12 maio 2004.

ROBIETTE, A. **BS7799 and other security frameworks**. 2003. Disponível em: <http://www.jisc.ac.uk/pub01/security_policy.html>. Acesso em: 22 maio 2005.

SANTILLO, L. **Common criteria or ISO 17799**. 2001. Disponível em: <http://www.sans.org/infoseqfaq/standards/iso17799.htm>. Acesso em: 14 jan 2006.

SANTOS, M. Práticas de gerenciamento estratégico da informação: como as empresas estão utilizando a informação para a competitividade. In: ENCONTRO ANUAL DA ANPAD, 28., 2004, Curitiba, **Anais...** Curitiba: ANPAD, 2004. 1 CD-ROM.

SCHMIDT, Howard. **Como garantir a segurança na Nova Organização**. Palestra ministrada no IT CONFERENCE, São Paulo, de 07 a 08 de jun. de 2006.

SOLMS, R.V. Information security management (2): the code of practice for information security management (BS7799). **Information Security & Computer Security**, Australia, v. 6, n. 5, p. 221-224, 1998.

STRONG, Diane M.; LEE, Yang W.; WANG, Richard Y. Data Quality in Context. **Communications of the ACM**, New York, v. 40, n. 5, p. 103-110, May 1997.

WILLIAMS, P. Information security governance. **Information Security Technical Report**, Oxford, v. 6, n. 3, p. 60-70, Sept. 2001.

YIN, Robert. **Estudo de casos**: planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2003.

BIBLIOGRAFIA CONSULTADA

BISSON, J.; SAINT-GERMAN, R. **Implementando políticas de segurança com padrão BS7799** / **ISO/IEC 17799:** para uma melhor abordagem da segurança da informação. 2006. Disponível em: <http://www.callio.com>. Acesso em: 27 maio 2005.

BRODBECK, A. F. **Alinhamento estratégico entre os planos de negócio e de tecnologia da informação**: um modelo operacional para a implementação. 2001. 319 f. Tese (Doutorado em Administração) – Programa de Pós-Graduação, Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2001.

CACIATO, Luciano E. **Gerenciamento da segurança da informação em redes de computadores e a aplicação da norma ISO/IEC 17799:2001**. 24 f. 2004. Monografia (Especialização em Análise de Sistemas) – Centro de Ciências Exatas, Ambientais e Tecnológicas. Pontifícia Universidade Católica de Campinas. Campinas, 2004.

CANEPA, Paola V. **Projeto de estruturação de um sistema de medidas de desempenho**. Porto Alegre: UFRGS, 2005.

DRUCKER, Peter F. **Desafios gerenciais para o século XXI**. São Paulo: Pioneira, 1999.

GUTEMBERG, Johann. **Museutec**. [S.l.] Disponível em: <http://www.museutec.org.br/linhadotempo/inventores/preview/johann_gutemberg.htm>. Acesso em: 7 ago. 2005.

KRAFTA, Lina; COSTA, Ricardo S. **Adequação de gestão da informação visando a efetividade da estratégia de ação comercial de pequenas empresas do ramo de TI**. [S.l.]: [S.n.], 2005.

LAUDON, Kennett C.; LAUTON, Jane P. **Sistemas de informação com Internet**. 4. ed. Rio de Janeiro: LTC. 1999.

LIMA, Luis F. Ramos. **Medindo a qualidade da informação no contexto brasileiro**: a situação da indústria bancária. Porto Alegre: UFRGS, 2005.

NERY, Felipe; PARANHOS, Mauricio. **COBIT ou ISO 17799?** Iniciando a reflexão. 2006. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 12 jul. 2005.

REDMAN, Thomas C. The impact of poor data quality on typical enterprise. **Communications of the ACM**, New York, v. 41, n. 2, p. 79-82, feb.1998.

ANEXOS

ANEXO A – RESOLUÇÃO 2.554-29/09/1998

Neste anexo serão transcritas as partes da Resolução cujos conteúdos estão relacionados com a Segurança da Informação conforme a seguir:

Resolução 2.554/1998 do Banco Central, que dispõe sobre a implantação e implementação de controles internos, especialmente:

> Artigo 1º - Determinar, às instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, a implantação e a implementação de controles internos voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis.
> [...]
> Artigo 2º - Os controles internos, cujas disposições devem ser acessíveis a todos os funcionários da instituição, de forma a assegurar que sejam conhecidas a respectiva função no processo e as responsabilidades atribuídas aos diversos níveis da organização, devem prever:
> [...]
> IV – a existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;
> V – a contínua avaliação dos diversos riscos associados às atividades da instituição;
> VI – o acompanhamento sistemático das atividades desenvolvidas, de forma a que se possa avaliar se os objetivos da instituição estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como a assegurar que quaisquer desvios possam ser prontamente corrigidos; e
> VII – a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.
> [...]
> Artigo 3º - O acompanhamento sistemático das atividades relacionadas com o sistema de controles internos deve ser objeto de relatórios, no mínimo semestrais, contendo:
> I – as condições dos exames efetuados;
> II – as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento das mesmas, quando for o caso; e
> III – a manifestação dos responsáveis pelas correspondentes áreas a respeito das deficiências encontradas em verificações anteriores e das medidas efetivamente adotadas para saná-las.
> [...]
> Artigo 4º - Incumbe à diretoria da instituição, além das responsabilidades enumeradas no art. 1°, parágrafo 2°, a promoção de elevados padrões éticos e de integridade e de uma cultura organizacional que demonstre e enfatize, a todos os funcionários, a importância dos controles internos e o papel de cada um no processo.

ANEXO B – INSTRUÇÃO CVM Nº 358-03/01/2002

Neste anexo serão transcritas as partes da Instrução cujos conteúdos estão relacionados com a Segurança da Informação conforme a seguir:

Instrução CVM n° 358, de 3 de janeiro de 2002, da Comissão de Valores Mobiliários, que dispõe, entre outros tópicos, sobre a divulgação e uso de informações sobre ato ou fato relevante, especialmente:

> Dever de guardar sigilo
> Artigo 8º - Cumpre aos acionistas controladores, diretores, membros do conselho de administração, do conselho fiscal e de quaisquer órgãos com funções técnicas ou consultivas, criados por disposição estatutária, e empregados da companhia, guardar sigilo das informações relativas a ato ou fato relevante às quais tenham acesso privilegiado em razão do cargo ou posição que ocupam, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo solidariamente com estes na hipótese de descumprimento.

ANEXO C – DECRETO Nº 4.553-27/12/2002

Neste anexo serão transcritas as partes da Decreto cujos conteúdos estão relacionados com a Segurança da Informação conforme a seguir:

Decreto n° 4.553, de 27 de dezembro de 2002, da Presidência da República, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, especialmente:

> Artigo 2º - São considerados originalmente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.
> Parágrafo único. O acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer.
>
> Artigo 3º - A produção, manuseio, consulta, transmissão, manutenção e guarda de dados ou informações sigilosos observarão medidas especiais de segurança.
> Parágrafo único. Toda autoridade responsável pelo trato de dados ou informações sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento."

O Artigo 4º, do Decreto acima citado, estabelece, entre outros, a definição dos seguintes itens:

> [...]
> VI – disponibilidade: facilidade de recuperação ou acessibilidade de dados ou informações;
> VII – grau de sigilo (confidencialidade): gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;
> VIII – integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;
> [...].

ANEXO D – DECISÃO QUANTO À CERTIFICAÇÃO

Com base no estudo elaborado por Fabio Ramos (2004), serão apresentados, a seguir, os fatores positivos a serem considerados quanto à decisão pela busca da certificação na *BS7799*:

- *aumenta a efetividade da segurança da informação*: a implementação do SGSI introduz o conceito de melhoria contínua através do *PDCA*. Esta sistemática provê a organização da capacidade de manter e monitorar de forma permanente as oportunidades de melhoria, e este é o aspecto mais importante da certificação;

- *investimento racional em segurança da informação*: em geral, as empresas não possuem suas necessidades de segurança claramente definidas e correm o risco de realizar investimentos de forma desordenada ou em valores acima do recomendado, tornando, desta forma, obscuro o retorno sobre os investimentos em segurança da informação. O SGSI permite identificar com maior precisão as necessidades de melhoria e onde seja mais necessário este investimento, garantindo um nível adequado de alinhamento entre segurança e necessidades da empresa;

- *diferencial de mercado*: em ambientes de forte concorrência ou baseados na confiança, tal como a área financeira, a existência do SGSI é um fator diferencial, percebido pelos clientes, fornecedores e órgãos reguladores. A *BS*7799 é uma poderosa ferramenta de marketing. Para o cliente, estar certificado pela *BS*7799 significa a tranqüilidade de saber que a empresa possui solidez no trato de suas informações, garantindo confidencialidade, disponibilidade e integridade;

- *gerar valor ao acionista e satisfazer requerimentos de clientes*: o SGSI é considerado um importante elemento complementar aos modelos de governança corporativa. Tendo-se o valor intrínseco da informação como um ativo intangível, a garantia de uma boa gestão de segurança da informação pode ser considerada uma medida tão importante quanto à da gestão de risco operacional, de crédito e de câmbio, entre outras;

- *único padrão com aceitação global*: a *BS*7799 representa uma convergência de interesses entre diversos tipos e portes de empresas, tanto na iniciativa privada quanto em empresas públicas, e é respeitada e reconhecida de maneira ampla;

- *pode gerar redução de despesas com seguros*: estar em conformidade com as práticas indicadas pela *BS7799* significa redução de riscos. Portanto, quanto menor o risco, maior a garantia de perpetuidade do negócio. Algumas empresas conseguiram expressiva redução nos prêmios de seguro, em vista da certificação;

- *cobertura das áreas de Tecnologia, Recursos Humanos e estrutura física*: a *BS7799* é uma norma com visão holística, considerando a proteção da informação, independentemente de sua apresentação física – digital, papel, voz, etc. – sob o ponto de vista tecnológico, administrativo e físico. De maneira equilibrada, a norma preocupa-se tanto com a vulnerabilidade de um funcionário insatisfeito, mas com grande conhecimento sobre informações da empresa, quanto com um equipamento de segurança com funcionamento inadequado;

- *reduz a probabilidade de risco devido à implementação de políticas eficientes*: a organização do SGSI através do modelo *PDCA* garante a continuidade de ações de segurança e a constante monitoração dos controles. Minimiza a necessidade de ação pontual contra focos de risco. As auditorias internas e o gerenciamento de incidentes garantem um tratamento contínuo das políticas de segurança;

- *a Alta Administração direciona as ações de segurança da informação*: com a estruturação do SGSI, segundo definido pela *BS7799*, quem direciona as ações táticas e operacionais de segurança da informação é o Fórum de segurança, composto majoritariamente pela Alta Administração;

- *revisão independente de seu SGSI*: a certificação na *BS7799*, recomendada por órgão certificador independente e outorgada por órgão internacional, atesta, de maneira imparcial, que o sistema implantado foi avaliado e atende aos requisitos estabelecidos na norma; e

- *certificação significa "due dilligence" e redução de risco*: estar certificado na *BS*7799 significa expressar publicamente que a organização realizou análise de risco das informações, possui uma política de segurança que foi amplamente divulgada, que existe uma sistemática de monitoração e correção de procedimentos com o objetivo de salvaguardar as suas informações.

ANEXO E – REQUISITOS E ETAPAS PARA A AUDITORIA DE CERTIFICAÇÃO

Uma vez definida a busca pela certificação, alguns itens devem ser atendidos para que a empresa possa submeter o seu SGSI à auditoria externa da *BS*7799, conforme a seguir:

a) a empresa deve concordar com o acesso aos registros do SGSI;
b) deve emitir a Declaração de Aplicabilidade;
c) deve definir o escopo de Certificação;
d) deve se submeter à Auditoria da metodologia;
e) deve se submeter à Auditoria do SGSI; e
f) deve se submeter à Auditoria periódica e reavaliação.

Uma vez cumpridas as etapas acima, para a realização da certificação, devem ser observadas as seguintes etapas:

a) assinatura do termo de confidencialidade;
b) pré-estudo de implementação do projeto de certificação;
c) pré-auditoria, realizada por auditoria homologada para a *BS*7799;
d) auditoria inicial, realizada por auditoria homologada para a *BS7799*;
e) atendimento às não-conformidades e/ou observações identificadas;
f) auditoria periódica, realizada por auditoria homologada para a *BS*7799;
g) recomendação para a Certificação;
h) outorga do Certificado por órgão certificador; e
i) auditoria periódica, realizada por auditoria homologada para a *BS*7799.

ANEXO F – EMPRESAS CERTIFICADAS

O Quadro 12 apresenta um panorama geral da *BS*7799 no mundo e no Brasil.

COUNTRY	NUMERO	COUNTRY	NUMERO	COUNTRY	NUM.
Japan	967*	Czech Republic	5	Chile	1
UK	210	Poland	5	Colombia	1
India	121	Switzerland	5	Egypt	1
Taiwan	56	Greece	4	France	1
Germany	40	Iceland	4	Lebanon	1
Korea	33	Spain	4	Lithuania	1
Italy	26	Brazil	3	Luxemburg	1
USA	23	Kuwait	3	Macau	1
Netherlands	21	México	3	Macedonia	1
Hong Kong	17	Saudi Arabia	3	Morocco	1
Australia	16	UAE	3	Qatar	1
China	14	Argentina	2	Romania	1
Finland	14	Belgium	2	Russian Federation	1
Hungary	13	Canadá	2	Slovenia	1
Ireland	11	Denmark	2	South Africa	1
Singapore	11	Isle of Man	2	Thailand	1
Norway	10	Malaysia	2	Turkey	1
Áustria	8	Slovak Republic	2	Relative Total	1697*
Sweden	7	Bahrain	1	Absolute Total	1685*

Quadro 12 – Número de Certificações em BS7799, por país[10]

Fonte: ISMS International User Group (2005).

Conforme se pode ver no Quadro 13, poucas empresas no Brasil possuem a certificação *BS*7799.

NAME OF THE ORGANIZATION	COUNTRY	CERTIFICATE NUMBER	CERTIFICATION BODY
Banco Matone S.A	Brazil	07502-2003-AIS-LDN-UKAS	DNV
Modulo Security Solutions S.A	Brazil	02154-2002-AIS-LDN-UKAS	DNV
Serasa, São Paulo	Brazil	262326 IS	DQS GMBH
Samarco	Brazil		

Quadro 13 – Número de Certificações em *BS7799* no Brasil

Fonte: ISMS International User Group (2005)

[10] *The Absolute Total represents the actual number of certificates (NOTE * includes the number of ISMS certificates in Japan only available in Japanese - please refer to the JIPDEC site of the listing ONLY in Japanese). *The Relative Total reflects certificates that represent multi-nation registrations or are dual-certifications. This table is copyright © ISMS International User Group 2001-2005.