CAROLINE ROGALSKY

IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE NECESSIDADES, CRIAÇÃO E AVALIAÇÃO DE UM PRODUTO DE INFORMAÇÃO

Monografia apresentada à disciplina de Projeto de Pesquisa em Informação II como requisito parcial à conclusão do curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientadora: Prof.ª Patricia Zeni Marchiori

CURITIBA

2005

Agradeço…

…a Deus,
pela Sua paz, que excede todo entendimento.

…a minha família,
pela paciência e compreensão.

…a professora Patricia,
pelo acompanhamento e orientação.

…aos meus colegas e demais professores da faculdade,
pelas inúmeras colaborações.

…aos profissionais entrevistados nessa pesquisa,
pelo tempo e atenção dedicados.

…a July,
pelo apoio moral e espiritual.

…a Gisah,
pela ação voluntária de revisar meu trabalho.

…aos amigos do *CADES*, especialmente do meu *P.G.*,
pelo incentivo e intercessão.

…a todos que, direta ou indiretamente,
contribuíram para a realização desse trabalho.

Porque o Senhor será a tua segurança
e guardará os teus pés de serem presos.

Provérbios 3:26

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

BSI – British Standards Institution

ISO – International Organization for Standardization

PDS – Plano Diretor de Segurança

SEC – Securities and Exchange Commission

SGQ – Sistema de Gestão da Qualidade

SGSI – Sistema de Gestão de Segurança da Informação

UFPR – Universidade Federal do Paraná

RESUMO

A segurança da informação torna-se cada vez mais necessária no âmbito empresarial, dado o aumento do compartilhamento de dados, especialmente por meio de redes de computadores. Porém, as condições de divulgação e sensibilização quanto ao tema são escassas, em particular na língua portuguesa, tendo como conseqüência o desconhecimento por parte das empresas. Procurando contribuir para a temática, se propôs a elaboração de um material de referência na área, que ilustrasse o processo de implantação de um Sistema de Gestão de Segurança da Informação (SGSI). Buscaram-se temas pertinentes na literatura, e aplicaram-se entrevistas em profundidade junto a profissionais de empresas de grande porte do município de Curitiba. Essas coletas de dados apoiaram a elaboração do material de referência que, durante o percurso do trabalho, se alterou de manual para um protótipo de guia. Este, por sua vez, foi submetido a avaliação pelos mesmos profissionais anteriormente entrevistados. Concluindo a pesquisa, as considerações finais foram redigidas, relacionando determinados comentários feitos pelos entrevistados a alguns aspectos abordados na literatura pertinente, descrevendo a vantagem da criação de um guia em detrimento de um manual, e também oferecendo diretrizes para continuação do trabalho e oportunidades de mercado para o gestor de informação.

Palavras-chave: Segurança da Informação; Sistema de Gestão de Segurança da Informação – SGSI; material de referência; guia de informação.

1 INTRODUÇÃO

Este trabalho de conclusão de curso se define como sendo um estudo de necessidades, seguido da criação e avaliação de um material de referência para implantação de um Sistema de Gestão de Segurança da Informação (SGSI).

Apresenta-se, num primeiro momento, o problema e sua justificativa, seguidos dos objetivos da pesquisa, o referencial teórico, a metodologia e os resultados alcançados.

Consistindo basicamente numa pesquisa de cunho exploratório, pois há poucos estudos anteriores que abordam o tema sob a ótica da Gestão da Informação, utilizou-se de métodos qualitativos, tais como a entrevista em profundidade que envolve maior esforço de análise. Com base nela e no levantamento de literatura pertinente gerou-se um protótipo de material de sensibilização e treinamento na área de segurança da informação, que pretende contribuir para ampliar o conhecimento da temática tanto no âmbito de empresas que buscam informações sobre a implantação de um SGSI, como da própria Gestão da Informação, enquanto área envolvida. Esse protótipo foi avaliado aplicando-se questionários, cujos resultados contribuíram para melhoria do material.

Concluindo o trabalho, as considerações finais relacionam alguns comentários dos entrevistados com certos aspectos abordados na literatura pertinente, descrevem a vantagem da criação do material de referência escolhido, e oferecem algumas sugestões de continuidade de trabalho e de oportunidades de mercado para o gestor da informação.

2 O PROBLEMA E SUA JUSTIFICATIVA

Contextualizando o cenário mundial DUPAS (1999, [f. 2]) relata:

> a partir do final da década dos 70 [sic], foram intensas as modificações socioeconômicas relacionadas ao processo de internacionalização da economia mundial. Desde já, é preciso enfatizar que esse processo não é novo. Mas ganhou características inusitadas e um assombroso impulso com o enorme salto qualitativo ocorrido nas tecnologias da informação. Essas mudanças permitiram a reformulação das estratégias de produção e distribuição das empresas e a formação de grandes *networks*.

Observa-se, nesse contexto, grandes empresas competindo para garantir a liderança tecnológica de produtos e processos, criando essas *networks* (redes globais), como também, empresas menores que vêm ganhando espaço através da onda de fragmentação (terceirizações, franquias e informalização) gerada pelas empresas maiores. Isso reflete as duas dialéticas centrais do capitalismo atual: "concentração *versus* fragmentação e exclusão *versus* inclusão" (id.). DUPAS pondera que, ao mesmo tempo em que se fala de inclusão no sistema global, há grande exclusão dos países em desenvolvimento que não conseguem alcançar os padrões impostos pelos desenvolvidos. E, mesmo dentro dos países em desenvolvimento, pode-se contemplar o reflexo desse problema mundial, visto que uma exceção consegue conquistar lugar no mercado e a outra parte vive buscando maneiras de sobreviver. Segundo DUPAS, "a disparidade de renda está crescendo, e a pobreza, o desemprego e o subemprego estão engrossando a exclusão social" (ibid., [f. 5]).

Dada esta realidade, o universo competitivo entre empresas que buscam conquistar a liderança no mercado que ocupam, exige que diversas medidas sejam tomadas. Dentre elas, há uma profusão de documentos descrevendo os mecanismos de planejamento estratégico para a ampliação das redes globais, destinados à parcela da população mais voltada para os meios de produção tecnológicos. O que sustenta o uso dessas redes é a informação que nelas circula – a veiculação e transferência de dados de empresas que, para dar continuidade aos seus negócios, tornam-se cada vez mais dependentes delas.

Em décadas anteriores à transferência das informações por esses meios, estas eram tratadas de maneira centralizada e pouco automatizadas. Havia muitas limitações e o preço dos primeiros *mainframes*[1] era muito alto. Logo, porém, os investimentos da indústria de alta tecnologia foram sendo amortizados e seus produtos se tornaram mais acessíveis. Os *mainframes* foram aos poucos assumindo a função de central de processamento e armazenamento de dados. Primeiramente, havia um único terminal por departamento e as consultas eram ainda remotas. Pouco mais tarde, como o compartilhamento da informação passou a ser considerado uma prática moderna e necessária de gestão, começaram a surgir as primeiras redes de computadores, tornando as informações ainda mais digitalizadas e os processos mais automatizados. Atualmente, pode-se contemplar as empresas aplicando as tecnologias da informação aos seus negócios num alto nível de conectividade e compartilhamento. O paradigma de acesso local à informação é quebrado com a presença de computadores em ambientes de escritório, cada vez mais portáteis, e com a utilização de uma grande rede como um dos principais meios de interação entre fornecedores, parceiros e clientes. Nesse cenário, percebe-se o alto grau de dependência das empresas em relação à informação – muito mais digitalizada, compartilhada e distribuída (SÊMOLA, 2003, p. 3-5).

Assim, cresce a importância das informações disponíveis nas redes, em especial daquelas que estão sob domínio de cada empresa, revelando a essência de suas linhas de negócios. Uma organização gera e acessa diversos tipos de informações, desde aquelas de cunho operacional e tático, até as consideradas estratégicas. Quanto mais valor é agregado à informação que produz, sua exposição ao mercado (especialmente concorrente) pode ser bastante delicada. A desvalorização da imagem de uma organização, a perda de mercado ou mesmo a descontinuidade dos negócios podem representar as conseqüências que a falta, ou má administração de informação que vise a segurança, pode acarretar.

[1] Computador de grande porte.

Considerando esse aspecto, uma pesquisa realizada no ano de 2004 no âmbito do curso de Gestão da Informação – Universidade Federal do Paraná (UFPR), junto a dez empresas de grande porte do município de Curitiba[2], apresentou alguns dos problemas na área da administração da segurança da informação. Dentre eles:

a) a visão da segurança da informação ainda limitada ao seu lado técnico;

b) a preocupação com os custos de investimento, ou seja, despesas que um projeto na área de segurança da informação pode gerar, e a conseqüente necessidade de racionalizar investimentos;

c) a falta de aplicação de procedimentos de segurança baseados na Norma ISO 17799[3], havendo apenas uma empresa (entre as dez que se voluntariaram a participar do estudo) que aplicava todos seus requisitos, e duas outras que apontaram apenas alguns itens que estavam sendo implementados. (DRAGO, 2004)

Uma vez que o tema "segurança da informação" se inseriu no âmbito da Gestão da Informação, e considerando esses problemas ainda existentes na área, pode-se aprofundar mais o assunto no que diz respeito ao processo de implantação de um sistema que vise a segurança da informação, abrindo possibilidades para a intervenção de um gestor.

Inicialmente, para que a administração da segurança de informação possa ser bem sucedida, é necessário atentar não apenas aos fatores tecnológicos, os quais são de

---

[2] O universo dessa pesquisa era de 22 empresas de grande porte do município de Curitiba, das quais apenas 10 concordaram em participar.

[3] A ISO 17799 – Código de Prática para a Gestão da Segurança da Informação, originou-se da Parte 1 da Norma Britânica BS7799 – Código de Conduta, sendo homologada pela *International Organization for Standardization* (ISO) em dezembro de 2000. A versão brasileira, foi homologada pela Associação Brasileira de Normas Técnicas (ABNT) em setembro de 2001, tendo uma versão atualizada no mês de agosto de 2005. A BS7799, por sua vez, foi publicada pela *British Standards Institution* (BSI), sendo divida em duas partes. Na Parte 1, que equivale a ISO 17799, é definido um código de prática para a gestão de segurança da informação. São as melhores práticas compreendidas em dez domínios, que se dividem em 36 grupos de controles e se desdobram em 127 controles finais, base para numerosas ações tecnológicas. A Parte 2 define um Sistema de Gestão de Segurança da Informação (SGSI), servindo de objeto para verificação de auditores e certificação (MÓDULO SECURITY, 200-). Essa parte da Norma também foi homologada pela ISO em 2005, consistindo na Norma ISO 27001.

inegável importância, mas também considerar os fatores humanos, uma vez que cada pessoa pode ser percebida como uma fonte de informação, e a sua conduta dentro e fora da empresa pode representar riscos e ameaças constantes.

Mais do que ter cautela com ambos os lados (humano e tecnológico) é essencial que haja o planejamento de um processo para implantação total de um Sistema de Gestão de Segurança da Informação (SGSI), a fim de evitar brechas que futuramente possam vir a causar danos à organização. Para tal, o instrumento de orientação definido oficialmente pela Associação Brasileira de Normas Técnicas (ABNT) é a ISO 17799 que, segundo GONÇALVES (2003), é atual e não se mantém somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação. Segundo a SYMANTEC (2002), a ISO 17799 é "…uma compilação de recomendações para melhores práticas de segurança, que podem ser aplicadas por empresas, independentemente do seu porte ou setor. Ela foi criada com a intenção de ser um padrão flexível, nunca guiando seus usuários a seguir uma solução de segurança específica em vez de outra". Para complementar essa Norma, foi homologada em 2005 pela *International Organization for Standardization* (ISO) a ISO 27001, consistindo no detalhamento dos estágios de desenvolvimento, implantação e manutenção de um SGSI. De modo geral, o objetivo principal dessas normas é contribuir para a garantia da segurança da informação das organizações, independente de seu porte.

Uma empresa que deseja proteger suas informações e, ao mesmo tempo, controlar os custos envolvidos na implementação de um SGSI, poderá comprar as Normas ISO e tomar para si a responsabilidade da implantação, ou então, contratar uma consultoria especializada. Todavia, ambas medidas podem não ter o sucesso desejado se a empresa não tiver uma orientação prévia e simplificada dos procedimentos envolvidos para implantação de tais Normas, bem como conhecer e/ou localizar ferramentas de apoio necessárias, uma vez que essas não são citadas nas Normas. Outro aspecto a ser considerado é que uma norma por si só não garante a

conscientização da empresa como um todo, uma vez que ela normalmente se encontra acessível apenas aos responsáveis pela segurança e, mesmo se fosse disponibilizada aos demais funcionários de uma organização, sua linguagem não lhes seria "amigável", nem a sua apresentação motivaria a leitura, entre outros fatores.

Considerando tais aspectos, poder-se-ia fornecer um meio de instrução e sensibilização anterior à implantação de um SGSI, que contivesse uma série de detalhes e especificações nas várias áreas que a implantação deste abrange. Este meio serviria para auxiliar a cooperação da empresa como um todo mediante a conscientização dos diversos aspectos envolvidos na segurança da informação de uma organização. Assim como, poder-se-ia encaixar no contexto intermediário ao das consultorias especializadas, uma vez que a empresa só poderá ter uma participação mais ativa no processo de implantação de um SGSI quando bem informada. Abre-se, desta forma, uma nova possibilidade para que a empresa reflita sobre seu ambiente organizacional, detectando peculiaridades e dinâmicas que um consultor pode não captar de imediato. Através de tal meio pode-se igualmente explicitar uma situação de seqüência de fatos que poderão ser vitais na visualização total da empreitada.

A definição de qual seria esse meio será baseada nos resultados da pesquisa do presente trabalho. Devido a isso, se utilizará, neste momento, o termo "material de referência" para se referir a ele. Uma vez definido esse material, um protótipo será construído e avaliado. Neste momento, serão abordados os objetivos da pesquisa e as idéias de alguns autores sobre os temas relacionados a esse trabalho.

3 OBJETIVOS

O trabalho de pesquisa a ser elaborado possui um objetivo geral que se desdobra em sete objetivos específicos.

3.1 OBJETIVO GERAL

Elaborar um protótipo de material de referência contendo procedimentos e fontes de informação relativos à implantação de um Sistema de Gestão de Segurança da Informação (SGSI).

3.2 OBJETIVOS ESPECÍFICOS

São objetivos específicos da pesquisa:

a) coletar informações relativas ao tema segurança da informação, implantação de um SGSI e consultoria em geral e na área de segurança da informação;
b) identificar tipologias relativas a materiais de referência;
c) definir a tipologia mais adequada para o protótipo;
d) verificar, junto a determinados profissionais de empresas de grande porte de Curitiba, as expectativas e necessidades relativas à criação de um material de referência para implantação de um SGSI;
e) verificar os procedimentos necessários para a implantação de um SGSI;
f) descrever sucintamente cada etapa do processo de implantação de um SGSI, especificando suas tarefas e fontes de informação relacionadas a cada uma delas – compondo desta forma, o conteúdo do protótipo;
g) submeter o protótipo à avaliação dos profissionais das empresas que participaram do levantamento de necessidades e expectativas em relação à criação de um material de referência na área de segurança da informação.

4 LITERATURA PERTINENTE

Nas próximas seções aborda-se o tema segurança da informação, apresentando suas características e a norma brasileira da área. Posteriormente, comenta-se sobre a implantação de um SGSI, a qual pode ser administrada por uma consultoria e/ou com o auxílio de um material de referência.

4.1 SEGURANÇA DA INFORMAÇÃO

Leis brasileiras que exigem das empresas a guarda de determinados documentos por certo período de tempo fazem da segurança da informação um quesito obrigatório no sentido de preservá-los. Além disso, uma informação de qualquer tipo pode consistir num ativo importante para os negócios, devendo ser protegida de forma adequada. Segundo a Norma ISO 17799, "a segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio" (ABNT, 2001, p. 2).

É importante salientar também que, segundo UEMURA (2005), "os objetivos nessa área não são só garantir o sucesso do negócio da empresa ou da iniciativa pública, é [sic] antes de tudo poder disponibilizar ao cidadão serviços com confiabilidade e alta disponibilidade". Ou seja, o cliente da empresa que protege suas informações deposita sua confiança nela, sendo ao mesmo tempo beneficiado pelos serviços de melhor qualidade. Isso é garantido pelas características de confidencialidade, integridade e disponibilidade das informações – foco da administração de segurança de informação. Segundo a ISO 17799, a confidencialidade é a garantia de que a informação só poderá ser acessada por pessoas autorizadas. A integridade refere-se à informação que é exata e completa. A disponibilidade é a característica que requer que a informação esteja acessível às pessoas autorizadas no momento em que for necessária (ABNT, 2001, p. 2). Somando a essas características,

OLIVEIRA (2005) apresenta o que chama de "tríplice PPT" – Pessoas, Processos e Tecnologias. Segundo o autor, a segurança da informação jamais será alcançada se esses três aspectos não estiverem envolvidos na estratégia de segurança. Cada uma dessas partes deve ser dosada de forma que haja um ponto de equilíbrio entre elas. Eis cada uma detalhada pelo autor:

> **Pessoas:** educação – o que fazer; treinamento – como fazer e conscientização – porque fazer. Já virou jargão no ramo da segurança: o elo mais fraco da corrente da segurança são as pessoas [sic]. É nas pessoas que começa e termina a segurança, basta que uma, na cadeia de processos não esteja preparada para que o risco de incidente aumente consideravelmente.
> **Processos:** estes devem ser flexíveis até o ponto que não afetem a segurança das informações, a partir daí devem ser tratados de forma rígida e metódica. Processos não podem ser engessados pelos controles e tecnologias, pois acabaria por causar a perda da agilidade e dinâmica da empresa, mas esta não deve ser mantida em detrimento da segurança. O equilíbrio deve ser buscado sempre.
> **Tecnologias:** A tecnologia só deverá ser aplicada onde puder suportar a Política de Segurança das Informações, as Normas e os Processos definidos para cumprimento da estratégia de segurança, e para reforçar o elo mais fraco da corrente, as pessoas. Se a norma diz que a estação de trabalho deve ser bloqueada na ausência do usuário, aplica-se a tecnologia para que o bloqueio seja automático em caso de falha humana (esquecimento do Ctrl+Alt+Del B – Bloquear Computador), por exemplo.

Todos esses e demais aspectos da segurança da informação precisam ser fundamentados quanto a procedimentos e controles. Em busca de tal fundamentação, pode-se encontrar algumas normas e documentos sobre o assunto, que buscam, orientar e detalhar cada aspecto para proteger informações. Por exemplo, existem as seguintes normas: *Orange book*, COBIT, BS 7799, entre outras.

Num pequeno relato histórico sobre o surgimento das normas de segurança, GONÇALVES (2003), cita alguns documentos e normas, voltadas na sua maioria para a segurança computacional. O *Orange Book*, segundo o autor, foi o marco zero de um processo mundial e contínuo de busca de medidas que garantissem a segurança de um ambiente computacional. Posteriormente, houve um esforço para a construção de uma norma que não se detivesse apenas à parte tecnológica da segurança, como também abrangesse a proteção de todas as formas de informação. De tal esforço resultou a Norma Britânica BS 7799. Como já mencionado, a Parte 1 desta Norma – Código de Conduta – deu origem à norma ISO 17799. Ressalta-se que "por se tratar de um código

de prática, esta parte da norma não é objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação" (SÊMOLA, 2003, p. 140). A Norma abrange 10 domínios (com 36 alvos de segurança e 127 controles) que são[4]:

a) política de segurança: elaboração de uma política que demonstre o apoio e comprometimento com a segurança da informação, bem como auxilie no direcionamento da gerência de segurança de informação, devendo ser revisada e avaliada periodicamente;
b) segurança organizacional: estruturação do gerenciamento da segurança da informação, definindo um fórum de gestão, funções e responsabilidades;
c) classificação e controle dos ativos de informação: elaboração de um inventário dos ativos de informação e determinação de seus proprietários responsáveis;
d) segurança em pessoas: educação e comunicação aos atuais e futuros funcionários sobre as expectativas da empresa em relação ao seu comportamento no que se refere à segurança de informações;
e) segurança física e do ambiente: orientações para proteção das instalações contra acessos não autorizados, danos e interferências;
f) gerenciamento das operações e comunicações: garantia de operação segura e correta dos meios de processamento de informações;
g) controle de acesso: monitoramento e controle de acesso aos recursos de informação;
h) desenvolvimento e manutenção de sistemas: toda infra-estrutura em tecnologia da informação existente ou a ser implementada deve ser pensada sob o ponto de vista da segurança da informação que deve garantir;
i) gestão da continuidade dos negócios: planos para proteção dos processos

[4] Paráfrase feita pela autora, baseada em leitura da NBR ISO/IEC 17799:2001.

cruciais que envolvem o negócio contra interrupções e continuidade das atividades do negócio;

j) conformidade: observação da compatibilidade do gerenciamento de segurança adotado pela organização com as leis, estatutos, contratos, entre outros vigentes em seu contexto.

Enfim, é imprescindível que uma organização, ao implantar seu SGSI, tenha conhecimento desses domínios e busque implementar os relativos controles de segurança de acordo com seu contexto. Todavia, antes de efetuar a implantação, é preciso planejá-la.

4.2 IMPLANTAÇÃO DE UM SGSI – ELEMENTOS BÁSICOS

SÊMOLA (2003, p. 86) afirma que o "planejamento é o fator crítico de sucesso para a iniciativa de gerir a segurança da informação". Para tanto, o autor sugere a criação de um Plano Diretor de Segurança (PDS), definido por ele como "a bússola que irá apontar o caminho e os passos (atividades) que irão formar o mosaico da solução e suprir as necessidades de segurança do negócio, conduzindo-o a operar sob risco controlado" (ibid., p. 87). O autor diz não haver um modelo de plano único capaz de ser implantado em qualquer organização, mas que cada uma deve considerar seu contexto, suas particularidades para modelar um plano personalizado (id.).

O PDS sugerido pelo autor, pode ser comparado ao planejamento do qual surgirá um SGSI, que segundo MACHADO (2004) é definido como "o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para segurança da informação".

É essencial que, no início da formulação do PDS, seja feito um diagnóstico – um levantamento das informações pertinentes ao negócio – e que se relacionem processos, aplicações e infra-estrutura física, tecnológica e humana (SÊMOLA, 2003, p. 87). Um novo sistema a ser integrado em uma organização, necessita estar em consonância com

os objetivos do negócio, do contrário, sua implantação não poderá ser bem-sucedida.

Dentre as etapas sugeridas por SÊMOLA para a estruturação de um PDS, salienta-se ser necessária, para os processos de um negócio, a estipulação de critérios que variam de "vitais" a "não consideráveis". Isso facilita a priorização de pontos de cobertura da segurança da informação. Uma vez observados os objetivos do negócio e os pontos críticos de seu processo, pode-se estruturar um planejamento para implantação de um SGSI que se alinhe a tais objetivos e contemple os aspectos mais vulneráveis, sensíveis e/ou importantes da organização (ibid., p. 90-91). Nesse planejamento, como em qualquer outro, é fundamental o apoio e a colaboração da alta gerência (ibid., p. 20-21). Ele deve ser composto de etapas estruturadas – considerando questões de tempo e recursos necessários e/ou disponíveis para atingir as metas estipuladas para a segurança da informação.

Em busca dessas etapas para planejar a implantação de um SGSI, encontraram-se alguns diagramas de blocos ou sugestões escritas de seqüências de procedimentos. A própria Norma BS 7799 – Parte 2 – , fornece seis passos para essa implantação:

a) definir as diretrizes da política de segurança da informação;
b) definir o escopo do SGSI;
c) fazer uma análise de risco;
d) definir os objetivos de controle e os controles propriamente ditos;
e) implementar controles;
f) fazer declaração de aplicabilidade (CAUBIT, 2002-2005).

Somando a essas etapas, CAUBIT (2002-2005) apresenta 15 passos para um projeto de implantação de um SGSI, baseados na implantação de um Sistema de Gestão da Qualidade (SGQ):

a) convencer a alta administração;
b) escolher o coordenador e a equipe de implementação;
c) escolher o órgão certificador;
d) avaliar a situação atual;
e) elaborar o cronograma de projeto;

f) fazer um nivelamento conceitual para toda a organização;

g) formar e implementar os grupos de trabalho;

h) estruturar a documentação do SGSI;

i) elaborar e implementar o manual da segurança;

j) efetuar um treinamento de suporte aos auditores internos;

l) promover auditorias internas de segurança da informação;

m) preparar a pré-auditoria;

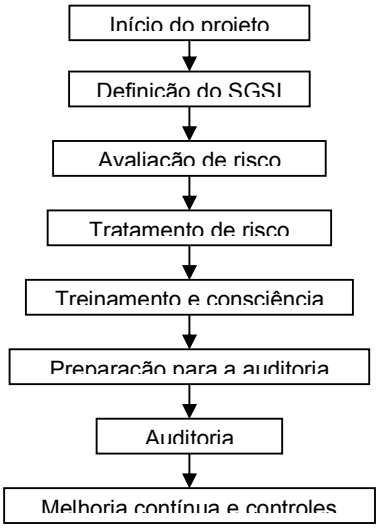
n) fazer a pré-auditoria;

o) efetuar disposições e plano de ação para as não-conformidades encontradas na pré-auditoria;

p) solicitar auditoria do órgão certificador.

Diferentemente dessas listagens de procedimentos apresentadas pela Norma e por CAUBIT, a empresa *Callio Technologies* [5] estruturou o seguinte diagrama de blocos:

FIGURA 1 – DIAGRAMA PARA IMPLANTAÇÃO DE UM SGSI DA CALLIO TECHNOLOGIES

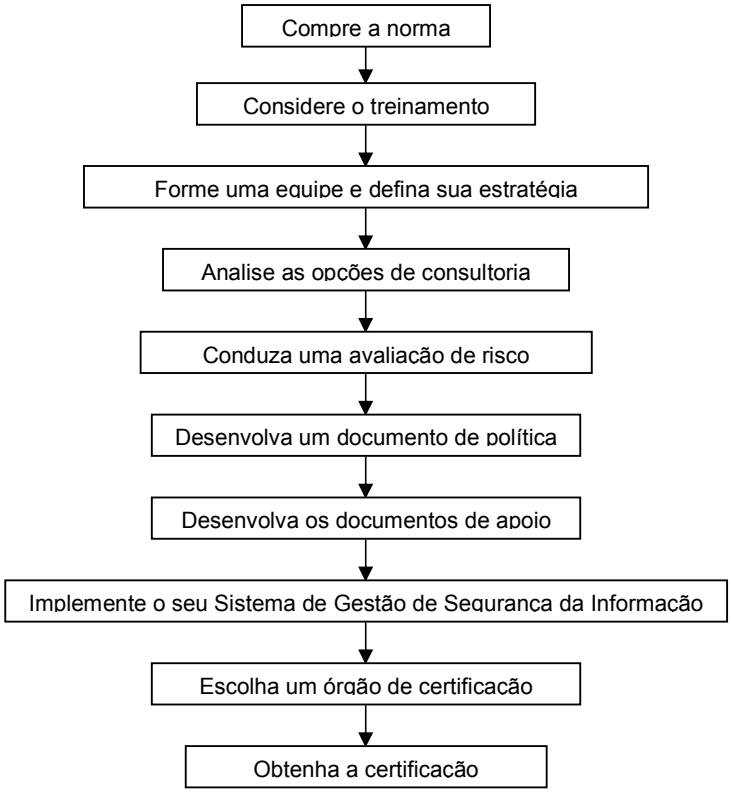


FONTE: BISSON, J.; SAINT-GERMAIN, R. **Implementando políticas de segurança com o padrão BS 7799/ISO 17799**: para uma melhor abordagem da segurança da informação. p. 12. Disponível em: <http://www.callio-pt.com/files/WP-ISO_PT.pdf> Acesso em: 22 mar. 2005.

[5] Empresa que oferece softwares que auxiliam o gerenciamento da segurança da informação em conformidade com a BS 7799 e a ISO 17799.

Além da *Callio Technologies*, outra empresa, a *BSI Management Systems*[6], elaborou um diagrama, que pode ser considerado mais completo que o anterior:

FIGURA 2 – DIAGRAMA PARA IMPLANTAÇÃO DE UM SGSI DA BSI MANAGEMENT SYSTEMS



FONTE: BSI Management Systems. **ISO 17799:** se sua informação não está a salvo, seu futuro não é seguro. Disponível em: <www.bsibrasil.com.br/Folder_ISO_17799_Port.pdf> Acesso em: 18 mar. 2005.

Apresentados esses quatro diferentes esquemas de procedimentos para implantação de um SGSI (da Norma BS 7799 – Parte 2 –, da autora CAUBIT e das empresas *Callio Technologies* e *BSI Management Systems*), fez-se uma comparação entre suas etapas. O Quadro 1 foi estruturado com a finalidade de agregar tais procedimentos e, posteriormente, auxiliar na descrição dos resultados desta pesquisa, e mesmo na construção de um novo e mais completo diagrama de blocos que poderá apoiar o material de referência a ser elaborado. A numeração existente nas células do quadro corresponde à ordem em que cada etapa se encontra na sua fonte original.

[6] Entidade certificadora da BS 7799.

QUADRO 1 – RELAÇÃO ENTRE DIVERSAS ETAPAS PARA IMPLANTAÇÃO DE UM SGSI

BS 7799 – PARTE 2	CAUBIT	CALLIO TECHNOLOGIES	BSI MANAGEMENT SYSTEMS
–	1. Convencer a alta administração	–	–
–	–	1. Iniciar o projeto	–
–	–	–	1. Comprar a norma
–	2. Escolher coordenador e equipe de implementação	–	3. Formar uma equipe e definir sua estratégia
–	–	–	4. Analisar opções de consultoria
–	5. Elaborar cronograma	–	–
1. Definir diretrizes da política de segurança da informação	9. Elaborar e implementar o manual da segurança	–	6. Desenvolver um documento de política
–	8. Estruturar a documentação do SGSI	–	7. Desenvolver os documentos de apoio
2. Definir escopo SGSI		2. Definir o SGSI	–
3. Fazer análise de risco	4. Fazer avaliação da situação atual	3. Fazer avaliação de risco	5. Conduzir uma avaliação de risco
4. Definir objetivos de controle e os controles	–	4. Tratamento de risco	–
–	6. Fazer nivelamento conceitual a toda organização	–	–
–	7. Formar e implementar grupos de trabalho	–	–
–	–	–	–
–	10. Treinamento de suporte a auditores internos	5. Treinar e conscientizar	2. Considerar o treinamento
5. Implementar controles 6. Fazer declaração de aplicabilidade	–	–	8. Implementar o SGSI
–	11. Executar auditorias internas	–	–
–	12. Preparar pré-auditoria	6. Preparar para auditoria	–
–	13. Fazer pré-auditoria	–	–
–	14. Considerar disposições e plano de ação para não-conformidades vistas na pré-auditoria	–	–
–	3. Escolha do órgão certificador	–	9. Escolher um órgão de certificação
–	15. Efetuar a auditoria do órgão certificador	7. Fazer a auditoria	–
–	–	–	10. Obter a certificação
–	–	8. Fazer melhorias contínuas e controles	–

FONTE: Adaptado de:

1. BISSON, J.; SAINT-GERMAIN, R. **Implementando políticas de segurança com o padrão BS 7799/ISO 17799**: para uma melhor abordagem da segurança da informação. p. 12. Disponível em: <http://www.callio-pt.com/files/WP-ISO_PT.pdf> Acesso em: 22 mar. 2005.
2. BSI Management Systems. **ISO 17799:** se sua informação não está a salvo, seu futuro não é seguro. Disponível em: <www.bsibrasil.com.br/Folder_ISO_17799_Port.pdf> Acesso em: 18 mar. 2005.
3. CAUBIT, R. **Como planejar e implementar a certificação BS 7799**, 2002-2005. Disponível em: <http://www.kcl.com.br/newkcl/informativos1.asp?id=761> Acesso em: 23 mar. 2005.

Verifica-se, no Quadro 1, que uma estrutura de etapas complementa a outra. A união das quatro colunas poderia representar uma seqüência de etapas mais completa que uma empresa poderá seguir no seu planejamento para implantação de um SGSI[7], fazendo-o por conta própria ou recorrendo a orientações de uma consultoria especializada. Nesse último caso, é importante que se conheçam as características básicas desse tipo de serviço no ramo da segurança da informação.

4.2.1 A Consultoria Como Elemento Auxiliar na Implantação da Segurança da Informação

WEINBERG (1990, p. XXI) define consultoria como "a arte de influenciar as pessoas que nos pedem [aos consultores] para fazê-lo. Quando as pessoas desejam algum tipo de mudança – ou temem algum tipo de mudança – procuram conselhos, de uma forma ou de outra". Ou seja, a consultoria está diretamente ligada à tomada de decisão relativa a mudanças que devem/precisam ser feitas numa empresa, tendo forte poder de influência.

DONADONE (2003, p. 1) especifica que "as empresas de consultoria despontam como um dos elementos de difusão e introdução de novos arranjos organizacionais, influenciando e, em muitos casos, direcionando a agenda dos possíveis formatos organizacionais". O mesmo autor destaca a questão de "um homem, uma idéia, uma nova consultoria", observada na criação de modismos e gurus gerenciais. Segundo ele, durante a década de oitenta há vários exemplos de pessoas que criavam e vendiam "pacotes gerenciais", ou seja, tinham grandes idéias e vendiam "fórmulas salvadoras de empresas". Nos anos noventa surgiram as ainda atuais críticas e questionamentos referentes à garantia de sucesso que tais pacotes prometem oferecer. Nesse período, também se colocou em cheque a questão ética e a facilidade de qualquer pessoa inexperiente poder ingressar no setor e se tornar um consultor,

[7] A união das etapas será fornecida nos resultados da pesquisa.

podendo causar graves danos a qualquer organização que a contratasse (ibid., p. 9-11).

Considerando tais aspectos negativos é importante, no caso de uma contratação, contemplar determinados adjetivos que uma consultoria de qualidade deve ter. No âmbito da segurança da informação, existem certas características desejáveis na consultoria externa, a saber:

- Posicionamento e perfil de Consultoria e Integradora de Ferramentas.
- Notória especialização em Segurança da Informação.
- Especificidade em Segurança da Informação.
- Equipe técnica multiespecialista.
- Ação local com visão global.
- Estrutura de execução de projetos capaz de viabilizar ações simultâneas em paralelo.
- Metodologia para dimensionamento de solução que considere fundamentalmente as características e desafios de negócio.
- Metodologia específica para execução de projetos de segurança da informação.
- Metodologias em conformidade com as normas internacionais BS7799 e ISO17799.
- Presença geográfica proporcional ou capaz de atender às características da empresa.
- Ponto de presença no exterior, viabilizando a absorção de experiências, inovações e tendências, e facilitação de parcerias e contatos técnicos.
- Comprovada experiência em projetos corporativos complexos. (SÊMOLA 2003, p. 68)

Considerando essas características, dentre os serviços e produtos oferecidos na área de segurança da informação, a empresa contratante pode optar por consultorias voltadas especificamente à área tecnológica – as quais vendem softwares de proteção antivírus, *firewalls*, criptografia, fazem testes de invasão a sistemas, entre outros – ou por consultorias especializadas na implantação da segurança da informação. Essas, por sua vez, além de realizarem avaliações tecnológicas, fazem análise de riscos, auxiliam na determinação de políticas de segurança e de planos de continuidade dos negócios. Algumas têm orientado programas de treinamento e/ou conscientização da segurança da informação dentro das empresas. As consultorias que se baseiam na norma BS 7799 ou em outra passível de certificação, também prestam serviços de auditoria, preparando as empresas para se tornarem certificadas.

Uma empresa interessada na implantação de um SGSI que opte por contratar alguma dessas consultorias, não terá que se preocupar em submeter grande parte do tempo de alguns de seus funcionários com todas as tarefas que envolvem a

administração da segurança da informação. Porém, pode querer e exigir da consultoria contratada um trabalho de qualidade, o qual só poderá ser avaliado mediante conhecimento da própria organização do que está sendo feito. Numa segunda hipótese, pode ser que a empresa queira ao invés de contratar uma consultoria, designar a funcionários específicos a função de administração da segurança da informação. Em ambos os casos, torna-se importante disponibilizar um material de referência, que some conhecimento e auxilie o processo de implantação de um SGSI.

4.2.2 Material de Referência para Implantação de um SGSI

Um termo similar a material de referência é o de "obras de referência ou fontes de referência" utilizado por DIAS (2000), cujo conceito se encaixa ao contexto do presente trabalho. O autor afirma que tais expressões "designam aquelas obras de uso pontual e recorrente, ao contrário de outras que são destinadas, normalmente, a serem lidas do princípio ao fim" (DIAS, 2000, p. 199). Cita como exemplo o dicionário "que ninguém lê do começo ao fim, mas a que se recorre, até mesmo diariamente, para procurar pequenas parcelas de informação, dentro do enorme conjunto de informações que esse tipo de obra normalmente contém" (id.).

Além deste, há vários tipos de materiais de referência citados por DIAS (2000) e também por PLACER (1968) – sob o termo "instrumentos de referência". Abaixo se listam os conceitos:

a) dicionário: "obra de referência que arrola, em ordem alfabética, as palavras de uma língua, das particularidades de uma língua, ou de assunto especial (ciência, técnica ou arte), com a definição, esclarecimentos gramaticais e outros" (PLACER, 1968, p. 41); exemplos: terminologias e glossários, bilíngües e poliglotas, de nomes, de abreviaturas (DIAS, 2000, p. 203-205);

b) tesauros: “listas de palavras de uma determinada área, apresentando o relacionamento entre os termos utilizados naquele assunto ou área do conhecimento” (ibid., p. 208);

c) enciclopédia: arrola “todos os ramos do conhecimento humano” (PLACER, 1968, p. 49), ou então, apresenta, “de forma concisa e facilmente acessível, informações a respeito do assunto de sua especialização” (DIAS, 2000, p. 209);

d) fonte biográfica: “é a descrição ou narração escrita da vida e obras de uma pessoa” (PLACER, 1968, p. 59);

e) fonte bibliográfica: “é o inventário tecnicamente anotado e sistematicamente classificado de material sobre um ou vários assuntos, numa ou várias línguas, apresentado num ou em diversos registros” (ibid., p. 70);

f) indicadores: “obras que proporcionam informações sobre pessoas, órgãos governamentais ou não-governamentais, instituições, sociedades, países ou determinado assunto especializado” (ibid., p. 83);

g) publicações oficiais (ou governamentais): “dimanam de governos nacionais, estaduais, provinciais ou municipais, tendo seus dados, porisso [sic], caráter legal” (ibid., p. 89);

h) publicações periódicas e seriadas: “publicações com título legal, de autoria vária, tratando de assuntos gerais ou especializados, com freqüência regular e periodicidade indefinida” (ibid., p. 95);

i) guias: “obras destinadas a proporcionar informações práticas (horários, logradouros, diversões etc.) e apontar as características notáveis (museus, bibliotecas, parques, monumentos, curiosidades etc.) de uma região, país, cidade etc.” (ibid., p. 101);

j) manuais: “obra compacta, que trata concisamente da essência de um assunto, tendo como finalidade principal servir como fonte de

informações correntes" (*GLOSSARY of library terms* apud DIAS, 2000, p. 210-211);

l) mapa: "representação sobre um plano, em escala reduzida, da superfície da terra ou parte dela" (PLACER, 1968, p. 107);

m) atlas: "uma coleção de mapas ou cartas" (id.).

Baseando-se nas definições apresentadas e considerando o objetivo principal do presente trabalho, descarta-se a possibilidade de usar alguns desses instrumentos, sendo eles:

a) dicionários: por se limitarem a oferecer definições de palavras e não a esclarecer profundamente um determinado tema – não fazem ligação entre conceitos;

b) tesauros: por se limitarem a relacionar termos;

c) enciclopédias gerais: por não tratarem de um assunto exclusivo (como no caso do presente projeto);

d) enciclopédias especializadas: por terem um "...nível altamente técnico" (DIAS, 2000, p. 209);

e) fontes biográficas: por serem descrições da vida e obras de uma pessoa;

f) publicações oficiais: por possuírem caráter legal;

g) publicações periódicas e seriadas: por possuírem autoria vária;

h) mapas e atlas: por serem documentos geográficos.

Dos conceitos que restaram, aquele apresentado para "guia" na visão de PLACER, refere-se a ele sob o ponto de vista de informação turística. Porém, numa definição mais atual, segundo CALDEIRA (2000, p. 263) guia é uma publicação que relaciona "fontes de informação relativas a um assunto, fornecendo uma visão geral da área abrangida e comentários a respeito das obras incluídas". Além disso, ele também traz informações sobre instituições da área que abrange. Tal definição engloba os outros dois conceitos restantes: de "fonte bibliográfica" (materiais sobre um ou mais assuntos organizados num ou mais registros) e "indicadores" (obras com informações sobre determinado assunto).

Outra opção restante é o termo “manual” que, segundo o dicionário HOUAISS (2001, p. 1842) é uma “obra de formato pequeno que contém noções ou diretrizes relativas a uma disciplina, técnica, programa escolar, etc.”; e “livro que orienta a execução ou o aperfeiçoamento de determinada tarefa (…)”. Um manual se aplicaria ao objetivo principal do trabalho no que diz respeito aos procedimentos relativos à implantação de um SGSI – pois, como diz o conceito, ele orienta a execução de uma tarefa. Porém, a criação de um material deste tipo redundaria no que é proposto na Parte 2 da Norma BS 7799[8], o que será explicado com detalhes nos resultados da pesquisa do presente trabalho.

Portanto, a definição que melhor se enquadra no objetivo principal do trabalho é a de “guia”, que pode orientar não só os procedimentos como também a localização de fontes de informação relativas à implantação de um SGSI, sendo assim mais completo que um manual e atingindo o objetivo de sensibilização e treinamento pretendidos.

Uma vez definido o instrumento de referência a ser utilizado é necessário saber como elaborá-lo.

4.2.2.1 Guia como material de referência

CALDEIRA afirma que os guias “pretendem abrir as portas da literatura para os usuários, especialmente aqueles que necessitam de informação para compreender as teorias e idéias que possam ser aplicadas em seus trabalhos” (CALDEIRA, 2000, p. 262), ou seja, um guia pode servir de auxílio na tarefa de implantação de um SGSI, trazendo informações e referências na área de segurança da informação.

Para construí-lo, LOBO e BARCELLOS (1992, p. 76) apresentam em seu artigo uma metodologia, composta das seguintes etapas:

[8] Ver nota de rodapé da página 4.

a) planejamento;

b) identificação, levantamento e coleta de informações;

c) automação;

d) edição do guia.

Na etapa de planejamento as autoras afirmam que devem ser definidos:

a) cobertura do guia, especificando a abrangência temática, geográfica e temporal;

b) tipos de informações que serão coletadas;

c) responsabilidades das entidades envolvidas;

d) estratégia de coleta;

e) instrumentos de tratamento da informação;

f) edição e distribuição do guia (id.).

Na fase de identificação, levantamento e coleta de informações LOBO e BARCELLOS sugerem uma série de procedimentos que devem ser executados, dentre eles: a elaboração de formulários para captação dos dados, estabelecimento de um cronograma, implantação de estratégia para coleta de informações, análise do tratamento do que foi coletado, digitação e correção das informações (ibid., p. 77).

No processo de automação do guia as autoras recomendam a utilização do aplicativo MicroISIS[9], o qual dispõe das funções de entrada e atualização dos dados, recuperação de informação, emissão de relatórios e importação/exportação de dados (id.).

Na última etapa, correspondente a edição do guia, deve-se considerar que ele é composto de um corpo, índice e lista de siglas de entidades. O corpo é formado de capítulos subdivididos em seções, sendo a ferramenta sugerida pelas autoras capaz de

[9] "O CDS/ISIS (MicroIsis) é uma tecnologia de tratamento genérico de informações desenvolvida e mantida pela Divisão de Informação e Informática da UNESCO, responsável pela sua manutenção e aprimoramento" (GRUPO SPISIS, 2000-2004). O Microisis não será utilizado no presente trabalho, uma vez que a pesquisa consiste na elaboração de um protótipo de um novo produto (incluindo seu leiaute, organização das informações, entre outros), não se baseando numa estrutura já pré-formatada, embora permita certa flexibilidade no armazenamento de dados.

produzir posteriormente o índice e a lista de siglas de entidades (ibid. 77-78).

Finda a criação do guia, este precisa ser avaliado e periodicamente revisto, uma vez que seu conteúdo necessita evoluir juntamente com a realidade que representa. Não foram encontrados critérios específicos para a avaliação de um guia, porém, há uma série de aspectos que podem ser de alguma forma mensurados, especialmente se ele for publicado em formato eletrônico.

4.2.2.2 Avaliação de guia em formato eletrônico

Uma vez que o guia pode ser disponibilizado por meio eletrônico, é possível adaptar critérios utilizados na avaliação de sistemas. DIAS (2002, p. 4) cita alguns deles relacionados à usabilidade, tais como: facilidade de uso e de reuso, eficiência, poucos erros, auto-aprendizagem, satisfação e prazer, percepção favorável do usuário.

Segundo a autora:

> a interface deve ser de fácil uso; o acesso às informações deve ser eficiente e deve requerer um mínimo de tempo e esforço dos usuários finais. O sistema de informações deve ser projetado de tal forma que os erros sejam minimizados e próximos de zero. O uso do sistema deve requerer pouco ou nenhum treinamento oferecendo interface intuitiva, permitindo a auto aprendizagem [sic]. O aspecto subjetivo da interface é igualmente importante determinando a usabilidade do sistema. (id.)

Ainda em relação à usabilidade, TORRES e MAZZONNI (2004, p.152) dizem que ela "pode ser mensurada, formalmente, e compreendida, intuitivamente, como sendo o grau de facilidade de uso desse produto para um usuário que ainda não esteja familiarizado com o mesmo". BARBOZA, NUNES e SENA (2000, p. 119) segundo a norma ISO 9241, afirmam que a usabilidade pode ser medida de três formas diretas, sendo elas: pela análise de suas características requeridas num contexto específico de uso, pela análise do processo de interação, e pela análise da eficácia e eficiência que resulta do uso de um produto.

Os mesmos autores levantam outros critérios de avaliação utilizados para *websites,* que também poderiam ser adaptados na avaliação de um guia. Eles

especificam “quatro dos sete quesitos apresentados no roteiro elaborado por Smith para *sites* informacionais: abrangência e propósito, conteúdo, planejamento visual/gráfico (*webdesign*), funcionalidade (interface e quesitos de navegação)” (ibid., p. 121). A abrangência e propósito se referem à amplitude ou limitação da fonte de informação – se foi rica ou não em detalhes, se deixou de mencionar alguma informação importante, se houve alguma restrição a informações. O conteúdo está relacionado com a escrita correta, a clareza do texto, entre outros. O planejamento visual/gráfico considera o aspecto visual, como tamanho das letras, cores, disposição da informação, etc. Quanto à funcionalidade, esta se relaciona à fácil navegabilidade e interface amigável.

Somando-se a todas essas idéias, pode-se ainda considerar numa avaliação os atributos que uma informação dita de qualidade necessita ter, alguns deles descritos por STAIR (2002, p. 6) e DAVENPORT (2002, p. 152-156):

a) exatidão: sem erros;
b) oportunidade: deve ser atualizada e estar disponível ao usuário no momento da sua necessidade;
c) acessibilidade: não ser de difícil e demorada obtenção; a interface para busca de informação deve ser compreensível, proporcionando facilidade para extrair o que é necessário;
d) envolvimento: a informação deve ser apresentada como útil;
e) aplicabilidade: quando a informação pode ser utilizada diretamente para equacionar problemas e auxiliar na tomada de decisão, sem que isso envolva mais análises e rearranjo de dados (o usuário deve poder ler sem precisar se empenhar para interpretá-la);
f) escassez: a raridade pode influir no valor, mas uma informação também pode ser valiosa mesmo não sendo rara; tal conceito também pode ser definido por uma informação nova ou não disponível para os concorrentes;

g) relevância: quando tem importância para quem vai usá-la;

h) flexibilidade: pode ser usada para diversas finalidades;

i) simplicidade: não pode ser exageradamente complexa;

j) verificável: oferecer ao usuário a capacidade de checar para saber se a informação está correta;

l) completa: contém todos os fatos importantes;

m) econômica: depende da relação custo-benefício.

Alguns desses critérios seriam mais fáceis para a mensuração que outros. Os itens escassez e economia, por exemplo, teriam certa complexidade na avaliação do material pelos usuários. Por isso, tendo concluído o guia, faz-se necessário avaliar quais dos critérios citados podem ser enquadrados em ferramentas de avaliação. Como uma dessas ferramentas pode-se destacar o questionário que, potencialmente, facilitaria o processo de mensuração das opiniões de diferentes usuários relativas ao guia, além de ser um meio rápido e prático para os respondentes que normalmente alegam não dispor de muito tempo. O questionário pode ser aplicado mediante acompanhamento do entrevistado durante a sua avaliação do guia, ou então, ser entregue juntamente com o material estipulando-se um prazo para resposta.

Ele deve ser elaborado considerando três objetivos a serem atingidos: “traduzir a informação necessária em um conjunto de questões específicas que os entrevistados possam e queiram responder; motivar os entrevistados a completarem a entrevista; e minimizar o erro de resposta” (MALHOTRA, 2001, p. 296). Isso depende da forma, ordem e maneira que as questões são redigidas, da escolha dos tipos de perguntas (abertas ou fechadas) e da aparência do questionário, levando em consideração a incapacidade e a relutância do entrevistado em responder. Depois de pronto é imprescindível submetê-lo a um pré-teste, a fim de eliminar quaisquer erros que possam ter passados despercebidos por quem o elaborou (ibid., p. 296-297).

5 PROCEDIMENTOS METODOLÓGICOS

Finalmente, depois de abordados os temas que envolvem a presente pesquisa, parte-se para a sua metodologia, que consiste em explicar como será feita a prática da teoria até então relatada.

Dentre os dois principais paradigmas de pesquisa citados por COLLIS e HUSSEY (2005, p. 54), pode-se dizer que a pesquisa, para a qual se desenvolveu a metodologia especificada adiante, foi mais fenomenológica (qualitativa) do que positivista (quantitativa). Isso se dá porque ela focou o significado e não a mensuração de um fenômeno social – nesse caso, as necessidades e expectativas em relação a um material de referência na área de segurança da informação.

Num primeiro momento, utilizou-se um método qualitativo de pesquisa: a entrevista em profundidade. Num segundo momento, utilizou-se um método quantitativo: um questionário. Porém, mesmo que esse método seja considerado quantitativo, sua avaliação se deu de forma qualitativa. As respostas dadas no questionário estavam intrinsecamente relacionadas à entrevista feita num momento anterior. Isso se explica pelo fato da entrevista ter visado um levantamento de necessidades e expectativas, e o questionário, a verificação da satisfação ou não delas. Foi necessária também uma revisão de literatura que embasasse os resultados obtidos por esses métodos, como também, o material de referência que se originaria deles.

Enfim, a metodologia que foi aplicada nessa pesquisa está apoiada nos objetivos específicos já explicitados (ver 3.2), podendo ser resumida nas etapas que seguem:

a) levantar informações relativas ao tema – segurança de informação – visando a criação de um protótipo de material de referência para implantação de um SGSI;
b) entrevistar profissionais de empresas de grande porte de Curitiba para levantar necessidades e expectativas quanto à criação desse material;
c) elaborar o protótipo de material de referência;

d) submeter o protótipo à avaliação, considerando a opinião dos profissionais que participaram das entrevistas;

e) analisar e comparar, quando apropriado, os resultados das entrevistas e da avaliação do protótipo feita pelos profissionais;

f) elaborar as considerações finais e sugerir continuidade da pesquisa no tema.

Na primeira etapa, coletou-se material referencial provindo de distintas fontes, eletrônicas e impressas (livros, pesquisas e trabalhos) sobre assuntos relativos ao tema segurança da informação (normas e notícias da área, procedimentos referentes à implantação de um SGSI, aspectos relacionados a controles de segurança, etc.), e sobre materiais de referência (quais os tipos, e como estruturar o material escolhido para o trabalho – no caso, o guia). Também se pesquisou algumas empresas de consultoria existentes na área e as suas linhas de trabalho.

Tais informações foram selecionadas e incorporadas no capítulo 4 – Literatura Pertinente, sendo algumas delas também utilizadas posteriormente para agregar conteúdo ao protótipo de material de referência.

Conjuntamente à coleta de informações, e utilizando o mesmo universo[10] de uma pesquisa acadêmica sobre segurança da informação realizada no curso de Gestão da Informação[11], empresas foram contatadas explicando-se os objetivos e a justificativa da pesquisa ao profissional responsável pela segurança da informação em cada uma delas, com a finalidade de solicitar sua colaboração através de entrevistas. Um roteiro de entrevista em profundidade foi elaborado (ver Apêndice 1), tendo como objetivo levantar as expectativas e necessidades desses profissionais em relação a um material de referência na área de segurança da informação. Nesse ponto, é importante salientar a observação feita por MALHOTRA (2001, p. 163): "mesmo que o entrevistador procure seguir um esboço predeterminado, o fraseado específico das

[10] 22 empresas de grande porte, de diferentes setores de atuação, do município de Curitiba.

[11] DRAGO, I. **Segurança da informação: estudo exploratório em organizações de grande porte do município de Curitiba.** Curitiba, 2004. 71 f. Monografia (Graduação em Gestão da Informação) – Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

perguntas e a ordem de sua formulação acabam sendo influenciados pelas respostas do entrevistado". Ou seja, o roteiro apresentado no Apêndice 1 serviu apenas como referencial, sendo adaptado de acordo com as respostas dadas pelos entrevistados.

Na época em que se elaborou o roteiro, tinha-se como objetivo a construção de um manual para implantação de um SGSI. Isso foi devido à dificuldade em encontrar material de sensibilização/treinamento na área de segurança da informação em língua portuguesa, e à constatação de que poucas empresas implantavam aspectos relacionados a essa mesma área. Posteriormente, baseando-se nos resultados das entrevistas (que foram gravadas e transcritas) somados às novas descobertas oriundas do levantamento de informações (que continuava ocorrendo conjuntamente), decidiu-se mudar o tipo de material de referência de manual para guia. As explicações detalhadas sobre essa mudança serão apresentadas nos resultados da presente pesquisa (ver 6.2.1).

Depois de concluídas essas primeiras etapas, e assumida a tipologia a ser desenvolvida (um guia), passou-se para a elaboração de seu protótipo, cumprindo os passos sugeridos por LOBO e BARCELLOS (1992, p. 76):

a) planejamento;
b) identificação, levantamento e coleta de informações;
c) automação;
d) edição do guia.

No primeiro passo (o planejamento), foi definida uma estrutura para o guia. Para determiná-la, considerando que o guia cobriria o tema "implantação de um SGSI", foram identificados alguns modelos de diagrama de blocos e/ou enumeração de etapas, que descreviam o processo de implantação de um SGSI. Após isso, estes foram avaliados, comparados e relacionados em suas etapas, o que resultou na definição de um novo diagrama (ver p. 37), tendo suas etapas ordenadas de maneira lógica e justificável. Essa estruturação foi necessária para, além de especificar a abrangência do guia, também facilitar a escolha dos tipos de informações que seriam coletadas para compor seu conteúdo.

Partindo para o segundo passo, realizou-se um levantamento de fontes de informação relativas a cada uma das etapas do diagrama dentro do prazo de um mês. Para tal, foram definidos critérios de qualidade e elaborados formulários para organizar a coleta de dados (ver 6.2.3).

Depois de identificar, levantar e coletar essas informações, descreveu-se brevemente cada uma das etapas do processo de implantação de um SGSI, destacando-se informações básicas relativas aos procedimentos a serem tomados em cada uma delas.

Já nos passos de automação e edição do guia, foi definido que ele estaria no formato de uma página *web*, visando facilitar o acesso por meio de *links* às fontes de informação disponibilizadas, assim como o acesso dos entrevistados ao conteúdo a ser avaliado. O programa utilizado para a montagem foi o *FrontPage*[12], por ser o único disponível para a aluna responsável pelo projeto. Um leiaute e uma interface amigável ao usuário foram esboçados (ver no Apêndice 2 o esboço definitivo). Um nome foi definido, sendo ele: "Guia de Fontes de Informação para Implantação de um Sistema de Gestão de Segurança da Informação – GeSec". Com base no esboço montou-se a estrutura do GeSec, preenchendo-a com as fontes de informação coletadas e a descrição feita para cada etapa do diagrama. Também foram elaborados textos correspondentes ao GeSec propriamente dito ("como usar", "metodologia", "contato", "glossário" e uma breve introdução). Para a construção do GeSec, ponderou-se as opiniões levantadas nas entrevistas feitas no início do projeto, bem como se consideraram antecipadamente alguns dos critérios de avaliação abordados no presente trabalho (ver 4.2.2.2), como, por exemplo, a usabilidade. Depois de pronto, o Gesec foi provisoriamente disponibilizado no endereço <http://geocities.yahoo.com.br/carolrogal>.

Após isso, estruturou-se um questionário baseado em técnicas de elaboração de instrumentos de coleta de dados. Cada uma de suas questões foi elaborada considerando pelo menos um dos critérios já mencionados anteriormente (ver 4.2.2.2), a saber:

[12] Ferramenta da *Microsoft Corporation* que objetiva a elaboração de páginas *web*.

a) abrangência e propósito: riqueza de detalhes, se o GeSec deixou de mencionar algo importante, se houve alguma restrição;
b) conteúdo: escrita correta, clareza do texto;
c) planejamento visual/gráfico: aspecto visual, como: tamanho das letras, cores, disposição da informação;
d) funcionalidade: fácil navegabilidade e interface amigável;
e) exatidão: sem erros;
f) envolvimento: a informação apresentada como sendo útil;
g) aplicabilidade: a informação podendo ser utilizada diretamente para equacionar problemas e auxiliar na tomada de decisão;
h) relevância: importância para quem vai usá-la;
i) simplicidade: a informação não ser exageradamente complexa.

Estruturado o questionário, fez-se um pré-teste com um profissional de mesma formação dos que compunham o universo da primeira entrevista. Com base nesse pré-teste, o questionário foi corrigido (ver versão final no Apêndice 3) e enviado aos participantes da pesquisa para que estes pudessem fazer uma análise do GeSec. Antes do envio, os colaboradores foram contatados por telefone, sendo informados do objetivo da avaliação e do prazo de entrega dos questionários preenchidos.

Como alguns dos participantes não retornaram o questionário dentro do prazo estipulado, esse foi estendido por alguns dias, sendo feita nova solicitação por telefone. Nos casos em que o participante não foi encontrado por esse meio enviou-se um *e-mail*.

Depois de terminado o prazo de devolução dos questionários – ainda que, dos seis entrevistados apenas quatro os devolveram –, fez-se uma análise das respostas. A partir dela, estruturou-se um relatório, o qual será apresentado nos resultados desta pesquisa.

Por fim, foram feitas as considerações finais, em relação à experiência proporcionada por este trabalho, bem como se deram sugestões para sua continuidade.

6 RESULTADOS DA PESQUISA

A seguir serão apresentados e descritos os resultados obtidos na execução da metodologia.

6.1 ENTREVISTA EM PROFUNDIDADE

O levantamento preliminar de informações sobre o tema de segurança da informação revelou pouco material na área e que, o existente abordava o assunto de modo genérico, em particular na língua portuguesa. Também em outro trabalho acadêmico realizado em 2004 no curso de Gestão da Informação – UFPR, verificou-se que apenas uma, das dez empresas que participaram da pesquisa, implantava os controles de segurança da norma ISO 17799, as demais tinham conhecimento escasso nessa área. Ponderando esses aspectos, considerou-se que um manual serviria como instrumento de orientação para os profissionais das empresas que desejassem implantar um SGSI e tivessem pouco ou nenhum conhecimento sobre o assunto.

Por isso, em entrevistas realizadas a seis profissionais de empresas de grande porte do município de Curitiba[13], buscou-se verificar suas necessidades e expectativas em relação à criação de um material de referência para implantação de um SGSI, mais especificamente, de um manual. Desses seis profissionais, cinco relacionaram suas idéias em relação a manuais às explicações de funcionamento que acompanham determinado equipamento ou sistema. Todos concordaram que um manual corresponde à estruturação de etapas para executar determinada tarefa. Quando se perguntou aos entrevistados se liam os manuais, dois afirmaram que sim, dois negaram e outros dois disseram que só lêem quando precisam de alguma informação específica. Dos que não lêem, um justificou-se dizendo que os manuais são muito extensos e possuem termos técnicos de difícil compreensão. Considerando os que só lêem quando

[13] Dos 22 profissionais (um de cada empresa contatada), seis deles, ou seja, 27,27% concordaram em participar da pesquisa.

precisam, percebe-se claramente a aplicação do conceito de DIAS (2000, p. 199) quando este afirma que os materiais de referência "designam aquelas obras de uso pontual e recorrente, ao contrário de outras que são destinadas, normalmente, a serem lidas do princípio ao fim".

Os entrevistados também consideraram as seguintes características negativas dos manuais: excesso de informação, falta de direcionamento e o fato de não serem elaborados para leigos (com a presença de termos técnicos que dificultam a compreensão, desmotivando a leitura).

Questionados sobre o que mudariam nos manuais, os entrevistados declararam, de maneira geral, que os fariam mais enxutos, elaborando-os com poucas páginas e enfocando os pontos críticos e complexos do tema a que se referirem. De forma mais breve, eles os elaborariam de maneira simples, objetiva e de fácil entendimento. Um deles sugeriu que os manuais fossem mais ilustrados e com menos conteúdo textual, outro porém, disse que não precisariam ter muitas figuras, bastavam ser bem escritos. Esse mesmo entrevistado citou como sendo fundamental que um manual contivesse um bom índice analítico, e apresentasse o assunto num processo, por ele chamado de "evolução gradativa", indo dos aspectos básicos aos mais complexos.

Já em relação ao que os entrevistados pensam sobre segurança da informação, apenas um deles ainda possuía a visão limitada aos aspectos técnicos, destacando a segurança da informação como a proteção contra *crackers,* suas invasões de rede, entre outros. Outro, por ser o único a trabalhar especificamente na área, ressaltou que a segurança envolve políticas, normas, procedimentos, controles, etc. Os demais igualmente mostraram domínio de conceitos mais amplos, considerando a segurança não só pelo seu lado técnico, como também o lado social, voltado às pessoas. Um dos entrevistados, que declarou já ter pesquisado sobre o assunto, afirmou que a área é muito vasta, sobre a qual ainda leu muito pouco.

Nenhum deles passou pelo processo de implantação de um SGSI. Apenas um participou da implantação de uma política de segurança. Este falou que numa próxima oportunidade usaria novamente as normas nas quais baseou sua experiência, porém daria mais atenção a detalhes e à interação com o usuário. Numa outra empresa estavam, no momento, planejando e implantando alguns controles de segurança da informação, mencionando que houve problemas com usuários que buscavam exceções naquilo que até então havia sido implantado. Outro entrevistado comentou que periodicamente faziam auditorias na empresa, mas relacionadas a segurança física da informação, como: ambientes de servidores trancados, proteção contra incêndios, controles de acesso, entre outros. Todos já alegaram terem sofrido algum tipo de ataque por falha na segurança na empresa.

Os entrevistados também foram questionados quanto ao que fariam na possibilidade de eles mesmos construírem um manual para implantação de um SGSI. Um deles disse que colocaria informações fundamentais. Outro, sugeriu uma introdução ao tema, sem envolver aspectos técnicos, porém ressaltando a importância da segurança da informação para o negócio. Um terceiro falou que estruturaria o manual em tópicos, abordando tanto aspectos técnicos quanto sociais da segurança. Dentre os assuntos sugeridos estavam: produtos da área, controles a serem implantados num projeto de segurança, custos e prós e contras da segurança da informação.

Quanto ao meio para publicação do manual, dois disseram ser interessante que fosse disponibilizado em meio eletrônico (intranet ou Internet), um sugeriu o formato impresso, e os outros três disseram ser ideal que fosse produzido em ambos.

Em relação às vantagens da criação de um material de referência desse tipo, os entrevistados citaram: a conscientização por meio de um material que não fosse técnico, a concentração de todos os aspectos envolvidos pelo tema num único local de pesquisa e um padrão que poderia servir como instrumento de orientação. Quanto a desvantagens, nenhuma foi citada.

De modo geral, percebeu-se que cada entrevistado ressaltou aspectos que, naquele momento, refletiam a principal preocupação de sua empresa. O primeiro entrevistado apresentou como característica forte a segurança física, estando, porém consciente de que todos os tipos de informação (para ele: digital e em papel) necessitavam de procedimentos de segurança (política da mesa limpa, cuidado ao repassar informações pelo telefone, etc.). O segundo demonstrou preocupação com normas a serem utilizadas dentro da empresa – restrições e liberações para usuários. O terceiro preocupava-se com a interação com o usuário, de modo que esse não visse a área de informática, responsável pela segurança na sua empresa, como inimiga. Mais especificamente, estava interessado na segurança interna, pois a externa alegava já estar bem protegida com a utilização de toda tecnologia disponível naquele momento. O quarto entrevistado ainda possuía uma visão bastante técnica da segurança da informação. Não comentou em nenhum momento o lado humano, principalmente interno. Já o quinto, demonstrava uma preocupação focada no negócio, como a proteção da marca da empresa, da sua continuidade, apesar de conhecer as várias normas existentes na área e possuir uma visão bastante holística da segurança da informação. O sexto e último entrevistado, estava engajado na reestruturação da parte de física da segurança da informação, mas mostrou-se mais preocupado com o que chamou de "segurança social"[14], a qual não sabia como deveria ser administrada.

Essas observações foram importantes para constatar que, considerando a falta de visão global da segurança da informação por alguns dos entrevistados, e o foco em apenas um de seus aspectos por parte de todos, um material de referência se tornaria deveras útil. Especialmente para demonstrar aquilo que poderia estar passando despercebido a esses profissionais no contexto de seu trabalho, bem como oferecer uma visão mais ampla dos processos que a segurança da informação envolve.

[14] Esse termo pode ter sido usado, supostamente, por influência de outro cada vez mais discutido dentro da área de segurança, que é a "engenharia social". Essa corresponde à atitude de pessoas mal-intencionadas que se valem da ingenuidade ou ignorância dos usuários para conseguir informações confidenciais, como senhas por exemplo (BEAL, 2005, p. 78).

Uma vez que as entrevistas foram analisadas, continuou-se com a coleta de informações sobre segurança da informação e seguiu-se para a etapa da criação do protótipo de material de referência.

6.2 ELABORAÇÃO DO PROTÓTIPO DE MATERIAL DE REFERÊNCIA

Para elaboração do protótipo de material de referência, foram desenvolvidas cinco tarefas: definição da tipologia, estruturação de um diagrama de blocos representando as etapas de implantação de um SGSI, coleta e descrição de fontes de informação relacionadas a elas e construção do protótipo propriamente dito. A seguir serão descritos os resultados obtidos na execução de cada uma dessas tarefas.

6.2.1 Definição da Tipologia

Ao fazer o levantamento de informações referentes ao tema segurança da informação, pensou-se, em princípio, em elaborar um manual para implantação de um SGSI. Tal hipótese foi cogitada devido à escassez de material de língua portuguesa na área e aos resultados obtidos em pesquisa realizada no âmbito do curso de Gestão da Informação – UFPR, a qual revelou que poucas empresas implementam alguns aspectos relacionados a esse tipo segurança. Como já mencionado anteriormente (ver 4.2.2), um manual, segundo dicionário AURÉLIO (1993, p. 350), é um "livro que traz noções essenciais sobre uma matéria". O dicionário HOUAISS (2001, p. 1842) oferece outras duas definições: "obra de formato pequeno que contém noções ou diretrizes relativas a uma disciplina, técnica (…)"; e "livro que orienta a execução ou o aperfeiçoamento de determinada tarefa (…)". Devido a essa característica, o manual pode ser utilizado como uma ferramenta auxiliar para direcionamento de tarefas, sendo justamente essa a intenção inicial do trabalho: direcionar a implantação de um SGSI.

Contudo, nas entrevistas realizadas, como também já relatado anteriormente, ouviram-se depoimentos que não justificavam a criação de um manual. Como por

exemplo, quando se perguntou aos entrevistados qual o significado pessoal que estes atribuem aos manuais, as respostas estavam ligadas a manuais de equipamentos e sistemas. Ao contrário dos conceitos apresentados nos dicionários, os entrevistados definiram manuais como sendo livros com informações detalhadas a respeito de procedimentos e tarefas, escritos de maneira bastante técnica e de difícil compreensão, ou seja, a idéia de manual pareceu não ter apelo suficiente em termos de atratividade para a leitura/consulta. Sendo assim, ele não atingiria o objetivo de sensibilização já mencionado.

Outro aspecto que justificou a não criação de um manual, foi a descoberta[15] da também já citada norma BS 7799 – Parte 2. Verificou-se que esta teria exatamente a mesma função, oferecendo o detalhamento das etapas para implantação de um SGSI, o que faria do manual um produto similar, que não somaria de maneira significativa na divulgação de conhecimento da área de segurança da informação.

Considerando as demais respostas dadas nas entrevistas, outro grande problema dos manuais é o excesso de informações. Um guia, segundo a definição dada anteriormente (ver 4.2.2.1), oferece uma visão geral do tema, ou seja, não é extenso e pode ser escrito de forma simples, objetivando a compreensão do usuário final e evitando esse excesso. O guia também engloba inúmeras fontes com uma breve descrição sobre elas, às quais o usuário pode se remeter caso queira, a fim de se aprofundar no conhecimento sobre o tema. Isso demonstra que um guia atingiria as vantagens descritas pelos entrevistados em relação à 'conscientização por meio de um material que não fosse técnico, a concentração de todos os aspectos envolvidos pelo tema num único local de pesquisa e um padrão que poderia servir como instrumento de orientação'.

Por isso, definiu-se, como material de referência a ser desenvolvido no presente trabalho, um protótipo de um guia de informação (o GeSec). E, para que este assumisse a funcionalidade de, ao mesmo tempo, sensibilizar e auxiliar a implantação

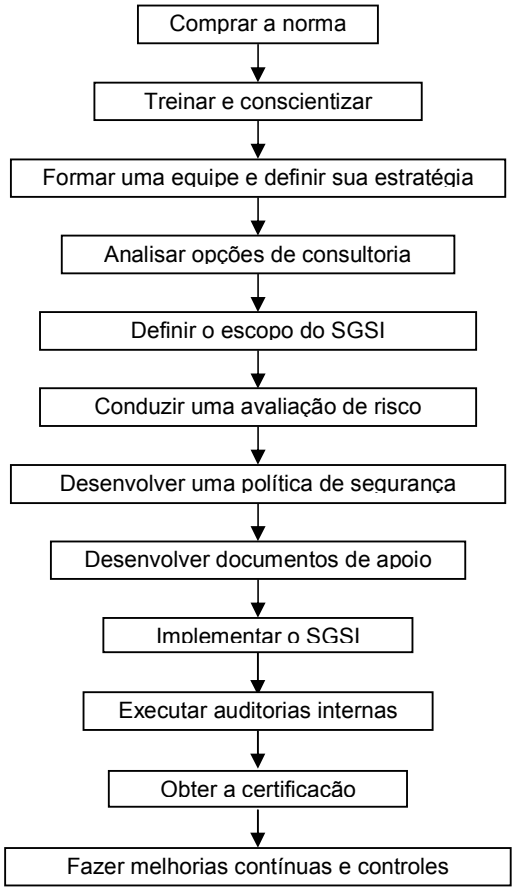
[15] A descoberta da BS 7799-2 e a definição da tipologia do material de referência ocorreram antes da homologação da ISO 27001, por isso essa Norma não é citada nessa parte do trabalho.

de um SGSI, foi necessária a estruturação de um diagrama de blocos que representasse as etapas dessa implantação e ao mesmo tempo fornecesse uma maneira lógica para organizar as informações contidas no GeSec e facilitar sua compreensão.

6.2.2 Elaboração do Diagrama de Blocos

No presente trabalho, foi apresentado o Quadro 1 (ver p. 15) que relaciona quatro tipos diferentes de ordenação de etapas para implantação de um SGSI. Com base nesse quadro construiu-se o seguinte diagrama para o GeSec:

FIGURA 3 – DIAGRAMA DE BLOCOS PARA IMPLANTAÇÃO DE UM SGSI



FONTE: Adaptado de:

1. BISSON, J.; SAINT-GERMAIN, R. **Implementando políticas de segurança com o padrão BS 7799/ISO 17799**: para uma melhor abordagem da segurança da informação. p. 12. Disponível em: <http://www.callio-pt.com/files/WP-ISO_PT.pdf> Acesso em: 22 mar. 2005.
2. BSI Management Systems. **ISO 17799:** se sua informação não está a salvo, seu futuro não é seguro. Disponível em: <www.bsibrasil.com.br/Folder_ISO_17799_Port.pdf> Acesso em: 18 mar. 2005.
3. CAUBIT, R. **Como planejar e implementar a certificação BS 7799**, 2002-2005. Disponível em: <http://www.kcl.com.br/newkcl/informativos1.asp?id=761> Acesso em: 23 mar. 2005.

Conforme se pode observar, foram excluídas as etapas apresentadas no Quadro 1: “convencer a alta administração” e “iniciar o projeto”. A primeira foi desconsiderada por não se tratar de uma questão relacionada diretamente ao processo de implantação de um SGSI (escopo do GeSec). Embora seja fundamental, o apoio da alta gerência precisa se concretizar antes do início do projeto de implantação e se manter durante todo o processo, por isso aparece no Quadro 1 antecedendo a etapa “iniciar o projeto”. Essa, por sua vez, foi eliminada por se tratar apenas de um tópico abordado sem maiores detalhes pela fonte consultada.

As etapas que se encontravam numa mesma linha do Quadro 1 foram consideradas como semelhantes, sendo aglutinadas. As demais etapas apresentadas no quadro que não apareceram neste diagrama foram inseridas em outras, como por exemplo: as etapas “elaborar o cronograma do projeto” e “formar e implementar os grupos de trabalho” foram consideradas como parte da etapa “formar uma equipe e definir sua estratégia”. A etapa “fazer um nivelamento conceitual para toda a organização” foi incorporada em “treinar e conscientizar”. As etapas “implementar controles” e “fazer declaração de aplicabilidade” foram consideradas como parte de “implementar o SGSI”. As etapas “preparar a pré-auditoria”, “fazer pré-auditoria”, “considerar disposições e plano de ação para não-conformidades encontradas na pré-auditoria”, “escolher o órgão certificador”, “efetuar auditoria”, foram englobadas em: “obter a certificação”, por serem tarefas diretamente relacionadas a essa última.

Uma vez definida a nova estrutura de diagrama de blocos, passou-se a coletar as informações que iriam compor seu conteúdo: as fontes e as descrições de cada uma das etapas para implantação de um SGSI.

6.2.3 Coleta de Fontes de Informação e Descrição das Etapas

Para coleta das fontes estabeleceu-se que estas deveriam estar disponíveis na Internet e que tivessem relação com alguma das etapas para implantação de um SGSI (incluindo materiais impressos, como livros por exemplo, que podem ser adquiridos

pela Internet, textos, artigos, bem como empresas de consultoria e entidades certificadoras da área que estivessem sendo divulgadas nesse meio).

Para organizar a coleta de dados, foi estruturado um formulário (ver Apêndice 4), que se baseou nos seguintes critérios de qualidade estabelecidos para a escolha das fontes virtuais (BIREME, 2002, p. 5-9):

a) periodicidade: se a fonte é atualizada;
b) acesso: se há ou não necessidade de uso de um *software* específico para acesso;
c) taxas/assinaturas: se a informação é disponibilizada gratuitamente ou se é necessário pagar por ela;
d) precisão: analisar se a fonte tem base científica e/ou em pesquisas, ou se é de opinião pessoal. Também verificar se já foi citada em outras publicações e se passou por um processo de revisão;
e) estabilidade da fonte: possibilidade de acesso permanente e constante à fonte de informação.

Considerando-se como exceções as fontes impressas que podem ser adquiridas através da Internet, foram avaliados apenas os critérios de periodicidade e precisão descritos acima.

Já para a seleção das consultorias foram utilizados os critérios definidos por SÊMOLA (ver 4.2.1). Sendo igualmente feito uma ficha de avaliação (ver Apêndice 5).

Ao se coletarem as informações, verificou-se que poucas delas se encaixaram dentro dos critérios estabelecidos. A princípio, buscaram-se fontes apenas no idioma português, mas, como foram encontradas poucas fontes consistentes, a pesquisadora optou por agregar algumas fontes em língua inglesa. Tal fato ocorreu especialmente para a etapa de certificação, uma vez que os órgãos certificadores identificados eram internacionais.

Depois de coletadas as fontes, e selecionadas apenas as que se encaixavam dentro dos padrões de qualidade estabelecidos, cada etapa do processo de implantação

de um SGSI, foi descrita sucintamente.

Considerando-se que o conteúdo selecionado era suficiente para sustentar uma primeira versão do GeSec, passou-se para a estruturação do protótipo propriamente dito.

6.2.4 Construção do Protótipo

O protótipo do GeSec (ver Apêndice 6) foi construído considerando antecipadamente alguns dos critérios de avaliação apresentados por DIAS (ver 4.2.2.2):

a) facilidade de uso e auto-aprendizagem: para o usuário compreender facilmente a ordem em que as etapas de implantação de um SGSI podem ser executadas e a lógica de sua ordenação, a seqüência dessas etapas foi claramente exposta em *links* na lateral esquerda da página; além disso, para eventuais dúvidas, foi formulado um texto auto-explicativo sobre como usar o GeSec, que pode ser acessado também através de *links* relacionados ao Guia propriamente dito;

b) poucos erros: o GeSec foi revisado e testado diversas vezes com o intuito de corrigir o maior número possível de erros;

c) satisfação e prazer: foram selecionadas cores amenas que não causassem desconforto ao usuário, como azul e cinza claros; os tamanhos, cores e tipos de letras também foram escolhidos considerando esse critério;

d) acesso eficiente às informações: os *links* destinados a páginas fora do GeSec remetem, sempre que possível, diretamente ao que se propõem;

e) mínimo de tempo e esforço dos usuários: os textos disponíveis no GeSec são curtos, rápidos e fáceis de entender; além disso, o usuário chega a uma fonte de informação com no máximo três “cliques”.

Além desses critérios também foram considerados os comentários feitos pelos entrevistados na entrevista em profundidade. Dentre eles, um material demasiado

longo e termos técnicos foram evitados, bem como o excesso de informação e a falta de direcionamento. O GeSec foi escrito de modo simples, com textos curtos de fácil compreensão, oferecendo direcionamento através da seqüência de etapas para implantação de um SGSI, a qual compõe sua estrutura. Já em relação à crítica sobre a maioria dos manuais não serem elaborados para leigos, a estruturação do GeSec levou em consideração que nenhum dos entrevistados – possíveis usuários do Guia – participaram de um processo de implantação de um SGSI, ou seja, são "leigos" no assunto. O GeSec também foi construído ponderando a maneira como os entrevistados disseram que elaborariam o material: de maneira enxuta, com poucas "páginas" e apontando diretamente os aspectos mais críticos e complexos do tema. Uma introdução ao tema (outra sugestão dada) também foi inserida ao conteúdo. Quanto ao meio para publicação do GeSec, como houve uma divisão equivalente de opiniões optou-se pelo mais prático para a pesquisa: o meio eletrônico. Enfim, a construção do GeSec buscou representar efetivamente, como já mencionado, as vantagens citadas pelos entrevistados: 'a conscientização por meio de um material não técnico, a concentração de todos os aspectos envolvidos pelo tema num único local de pesquisa e um padrão que poderá servir como instrumento de orientação'.

Terminado o protótipo do GeSec, passou-se para o processo de sua avaliação.

6.3 AVALIAÇÃO DO PROTÓTIPO

Considerando os questionários de avaliação do protótipo do GeSec enviados aos seis participantes da primeira entrevista, apenas quatro retornaram o questionário respondido.

As primeiras questões estavam relacionadas à aparência do GeSec.

Em relação ao título do Guia e aos *links* fixos situados à esquerda da página do protótipo, todos responderam que o estilo de letra era adequado e a cor era agradável. Já em relação ao tamanho, três responderam que era adequado e um respondeu ser inadequado. Esse entrevistado sugeriu que os *links* fixos à esquerda poderiam ter letras

maiores e destacadas, sem estarem sublinhados.

Quanto ao conteúdo central (o texto principal) e a janela correspondente à lista de fontes de informação, todos responderam que as letras tinham estilo e tamanho adequados e sua cor era agradável.

As cores de fundo do GeSec também foram consideradas por todos como agradáveis. E a maneira como a informação foi organizada, adequada. Vale ressaltar que nessa questão nenhum dos entrevistados marcou a opção "totalmente adequada".

Incitados a darem críticas e sugestões em relação à aparência geral do GeSec, um dos entrevistados afirmou que o Guia "está bem organizado e intuitivo, muito bom". Outro escreveu que está "simples e direto" e que "ficou agradável".

Depois das questões relacionadas à aparência do GeSec, foram feitas perguntas quanto à usabilidade (facilidade de uso) dele.

Todos os entrevistados afirmaram que o Guia permite a auto-aprendizagem, ou seja, conseguiram entendê-lo por si mesmos.

Questionados quanto ao Guia estar livre de erros, dois responderam positivamente e dois preferiram não opinar.

Já com relação às questões concernentes ao conteúdo do GeSec, na primeira delas os entrevistados afirmaram que os textos, de modo geral, estão escritos de forma clara, de fácil compreensão. Todos igualmente confirmaram que o GeSec cobriu toda informação que consideram importante. Porém, numa das questões abertas posteriores, um dos entrevistados sugeriu que fossem abordados os assuntos: "Plano de Continuidade de Negócios"[16] e "Lei Sarbanes-Oxley"[17].

---

[16] Também conhecido como Plano de Contingência, esse assunto está inserido na Avaliação de Risco (sexta etapa da implantação de um SGSI, segundo diagrama elaborado no presente trabalho). Consiste num plano que deve "garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre" (SÊMOLA, 2003, P. 98).

[17] Lei americana de reforma corporativa promulgada em 2002, após a ocorrência de vários escândalos contábeis, para dar maior publicidade às informações e propiciar fiscalizações preventivas pela SEC (*Securities and Exchange Commission* – Comissão de Valores Mobiliários dos Estados Unidos). O objetivo principal dessa lei é coibir a conduta antiética de administradores e auditores. Ela surgiu para restaurar a confiabilidade nas demonstrações contábeis e financeiras, e com isso incentivar o investimento na Bolsa de Valores (LIMA, 2004).

Quando questionados se as informações contidas no Guia facilitaram a percepção da segurança da informação no contexto da empresa onde trabalham, isto é, se eles perceberam aspectos que tem sido ou que faltam ser implementados nas suas organizações através do GeSec, três responderam que sim, e o outro, não.

As mesmas respostas foram observadas quando se perguntou se as informações contidas no GeSec poderiam de alguma forma auxiliar os entrevistados na tomada de decisão em relação aos aspectos que a segurança da informação envolve nas suas empresas.

Das críticas e sugestões dadas pelos entrevistados ao conteúdo do GeSec, o que respondeu negativamente às duas questões anteriores sugeriu: “o conteúdo precisa ser mais rico, ou definir qual a estratégia do mesmo”. Em outra resposta esse mesmo entrevistado sugeriu: “o Guia precisa ser informativo ou técnico. Se ele for apenas para o conhecimento inicial, ele atende às necessidades propostas, caso contrário, será necessário colocar informações complementares no Guia”. Um outro escreveu: “achei o Guia bem prático e de fácil entendimento, fazendo com que os gestores das empresas, que não possuem o conhecimento técnico em questão, possam estar cientes dos riscos que correm se não se preocuparem em implementar um SGSI”. Esse mesmo entrevistado escreveu: “acho que esse Guia é uma boa ferramenta para que as organizações observem a importância da implementação de um SGSI”. Um terceiro afirmou que o Guia “trata do assunto, num primeiro momento, de uma forma clara e abrangente, dando ao seu leitor toda a idéia das etapas a serem cumpridas. Contudo, no caso de um trabalho efetivo, faz-se necessária a busca de matérias mais profundas”.

Em relação a essas observações, torna-se importante salientar que o entrevistado que respondeu negativamente já possui um conhecimento mais abrangente na área de segurança da informação, embora nunca tenha implantado um SGSI. Já os outros três não têm esse mesmo conhecimento. Isso refletiu que o GeSec atingiu seu objetivo, uma vez que deveria sensibilizar e oferecer uma orientação para aqueles que buscam conhecimento na área, e por esses foi aprovado. Ele em si, não

poderia se aprofundar demasiadamente no assunto, uma vez que as fontes apontadas nele têm esse objetivo. E justamente por isso, essas fontes de informação – "as matérias" citadas pelo último entrevistado – num trabalho efetivo (num guia completo, não num protótipo como esse), devem ser mais profundas, exigindo uma busca mais demorada e específica daquele que o editar.

De modo geral, pode-se dizer que a avaliação foi positiva e que o GeSec – ainda que na forma de um protótipo – pode suprir as necessidades levantadas pelas empresas na entrevista em profundidade, uma vez que essas se sentiram satisfeitas com seu formato e conteúdo.

Terminada a avaliação do GeSec, segue-se para o que foi observado durante o desenvolvimento do presente trabalho, bem como sugestões para sua continuação.

7 CONSIDERAÇÕES FINAIS

O presente trabalho buscou aliar a teoria com a prática, mediante o levantamento de literatura pertinente na área de segurança da informação e à aplicação de uma pesquisa qualitativa, ambas com a finalidade de elaborar e avaliar um produto informacional.

Durante o período de coleta de informações sobre o tema de segurança da informação chamou grande atenção a escassez de material, especialmente em língua portuguesa, sobre o assunto. Já os resultados apresentados em um trabalho acadêmico do curso de Gestão da Informação – UFPR (feito no ano anterior ao da presente pesquisa), apontavam a falta de um conhecimento sólido sobre o tema pelas empresas participantes. A escassez de material somada a esses resultados, mostrou claramente uma "brecha" de trabalho para o gestor: reunir a informação que se encontra rara e fragmentada com o objetivo de oferecê-la a quem não a possui, no formato de um material de referência. Entretanto, os não possuidores dessa informação poderiam não perceber essa necessidade própria. Por isso, uma entrevista em profundidade foi aplicada utilizando intencionalmente o mesmo universo de pesquisa do trabalho feito anteriormente, verificando as reais necessidades e expectativas em relação a um material de referência na área de segurança da informação, naquele momento definido como um manual.

Porém, na continuação da coleta de informações, a descoberta de uma norma britânica (a BS 7799, em especial sua Parte 2) foi, em grande parte, responsável pelo redirecionamento do trabalho, o qual inicialmente tinha como objetivo a construção de um manual, sendo alterado para a elaboração de um guia. No entanto, mesmo que essa mudança tenha ocorrido após a aplicação da entrevista em profundidade, não prejudicou a continuação do trabalho. Muitos dos resultados levantados nessa primeira pesquisa puderam ser adaptados e, inclusive, justificaram a construção do protótipo de guia – o nomeado GeSec. Dentre as críticas e sugestões levantadas, foram evitados na

construção do GeSec: o excesso de informações, a linguagem técnica e a falta de direcionamento. Isso teve embasamento na literatura pertinente sendo relacionado aos critérios de avaliação: facilidade de uso e auto-aprendizagem. O excesso de informações poderia prejudicar o fácil uso do guia, e a linguagem técnica comprometeria a compreensão do produto e, conseqüentemente a auto-aprendizagem. Essa também poderia ser prejudicada pela falta de direcionamento, a qual se evitou com a utilização de uma seqüência de etapas para compor a estrutura do GeSec. A adaptação dessa seqüência teve origem também na literatura, com base em quatro esquemas diferentes que tiverem seus passos avaliados.

De modo geral, a elaboração do GeSec supriu, segundo a avaliação feita através dos questionários aplicados junto aos profissionais participantes da pesquisa, as necessidades e expectativas anteriormente levantadas, uma vez que a maioria das respostas foi positiva. Também não houve, nesse momento, nenhuma crítica sobre algum aspecto negativo relatado na primeira pesquisa – a entrevista em profundidade.

O GeSec também se adequou de forma mais apropriada a essas necessidades, do que um manual se adequaria. Pode-se verificar isso, fazendo-se um cruzamento entre as necessidades e expectativas dos entrevistados com as características de cada um dos materiais. Segundo os entrevistados, os manuais são extensos. Um guia, do contrário fornece uma visão geral de um tema, não tão detalhada quanto um manual. Essa visão geral também se adequou ao comentário feito por um dos entrevistados que pesquisou sobre o assunto de segurança da informação, e disse que esse tema abrange muitos aspectos que na sua maioria ainda desconhece. Num manual a abordagem desses variados aspectos faria com que sua extensão se alongasse, já no guia, os diversos assuntos podem ser apontados de forma geral, oferecendo ao usuário a opção de se aprofundar no que for de seu interesse a partir das fontes de informação indicadas. Outro aspecto interessante é que nenhum dos entrevistados passou pelo processo de implantação de um SGSI. Com um manual eles partiriam diretamente para a prática – uma vez que ele se limita a oferecer as diretrizes para execução da tarefa, já

o guia, ao mesmo tempo em que pode direcionar as tarefas, é um meio que fornece ao usuário a oportunidade de se informar mais sobre o assunto antes de colocá-lo efetivamente em prática. Com relação à citação feita nas entrevistas sobre ser um padrão de orientação, o manual se enquadraria, porém, poderia haver certa inflexibilidade causada pelo detalhamento das tarefas, que talvez não se adequaria a todo tipo de organização. O guia, por outro lado, oferece direcionamento – aponta o que precisa ser feito – sem ser específico em demonstrar "como fazer", indicando fontes que ensinam a fazer de diferentes modos, tendo, dessa forma, flexibilidade de adaptação das organizações ao seu contexto.

Enfim, o GeSec consiste num protótipo cuja criação se baseou totalmente nas pesquisas realizadas – entrevistas em profundidade, levantamento referencial e questionários de avaliação.

Contudo, deve-se destacar que foram coletadas informações e opiniões de seis profissionais na entrevista em profundidade (de 22 empresas contatadas) e, destes seis, apenas quatro responderam ao questionário de avaliação. Ainda que não se tenha proposto um trabalho quantitativo (no qual as condições de representação estatística colocariam em risco as generalizações), pode-se dizer que as respostas obtidas direcionam a avaliação do produto em um primeiro momento, não sendo todavia, definitivas ou conclusivas sobre a qualidade do GeSec em seu aspecto formal e de conteúdo.

Visando oferecer sugestões de continuidade deste trabalho, além de uma avaliação mais profunda e a construção de um guia completo (incluindo fontes de informação mais específicas), sugere-se que possam ser formuladas metodologias flexíveis para a gestão da segurança da informação dentro de cada etapa que a implantação de um SGSI abrange. Outra sugestão seria de discutir diretrizes para o cálculo de custos envolvidos num projeto de implantação de um SGSI, uma vez que isso pode ser fator importante para a aprovação da alta administração de uma organização. Também seria interessante que se discutisse o papel específico do gestor

da informação e seu inter-relacionamento com os demais profissionais que poderiam compor uma equipe de segurança, cada qual com uma função específica.

Como a segurança da informação é assunto recente, conforme se observou ao coletar informações, em muito o gestor da informação pode se envolver nessa área, não só auxiliando no âmbito da pesquisa, como também emergindo no mercado. Partindo desde a conservação da informação (tarefa relacionada a arquivística), passando por sua classificação (utilizando métodos específicos), como também pelo diagnóstico do fluxo dessa informação, o detalhamento das tarefas dos diferentes departamentos de uma organização, dentre outros aspectos que se relacionam direta ou indiretamente com a segurança da informação e que são estudados durante o curso daqueles que se graduam como gestores. O mercado é recente e amplo, e o perfil desse profissional tem chances significativas de ser aproveitado.

REFERÊNCIAS

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

BARBOZA, E. M. F.; NUNES, E. M. de A.; SENA, N. K. *Web sites* governamentais, uma esplanada à parte. **Ciência da Informação,** Brasília, v. 29, n. 1, p. 118-125, jan./abr. 2000.

BEAL, A. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p.

BIREME; OPAS; OMS. **Metodologia LIS:** critérios para seleção de fontes de informação em saúde disponíveis na Internet. (S.n.: s. l.), 2002.

CALDEIRA, P. da T. In: CAMPELLO. B. S.; CENDÓN, B. V.; KREMER. J. M. (Org.). **Fontes de informação para pesquisadores e profissionais.** Belo Horizonte: UFMG, 2000. p. 263-274.

CAUBIT, R. **Como planejar e implementar a certificação BS 7799**, 2002-2005. Disponível em: <http://www.kcl.com.br/newkcl/informativos1.asp?id=761> Acesso em: 23 mar. 2005.

COLLIS, J.; HUSSEY, R. **Pesquisa em administração:** um guia prático para alunos de graduação e pós-graduação. 2. ed. Porto Alegre: Bookman, 2005. 712 p.

DAVENPORT, T. H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. 5. ed. São Paulo: Futura, 2002. 316 p.

DIAS, E. W. In: CAMPELLO. B. S.; CENDÓN, B. V.; KREMER. J. M. (Org.). **Fontes de informação para pesquisadores e profissionais.** Belo Horizonte: UFMG, 2000. p. 199-216.

DIAS, R. Métricas para avaliação de sistemas de informação. **Revista Eletrônica de Sistemas de Informação,** v. 1, n. 1, nov. 2002. Disponível em: <http://www. presidentekennedy.br/resi/edicao1.html> Acesso em: 08 jun. 2005.

DONADONE, J. C. O mercado internacional de consultorias nas últimas décadas: crescimento, diversificação e formas de disputa. **Caderno de Pesquisas em Administração**, São Paulo, v. 10, n. 2, p. 1-15, abr./jun. 2003.

DRAGO, I. **Segurança da informação: estudo exploratório em organizações de grande porte do município de Curitiba.** Curitiba, 2004. 71 f. Monografia

(Graduação em Gestão da Informação) – Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

DUPAS, G. **Globalização, exclusão social e governabilidade.** Trabalho apresentado na 1. Conferência Latino-americana e Caribenha de Ciências Sociais, Recife, 1999. Disponível em <http://www.fundaj.gov.br/clacso/paper12.doc> Acesso em 21 mar. 2005.

GONÇALVES, L. R. de O. **Pequeno histórico sobre o surgimento das normas de segurança,** 18 ago. 2003. Disponível em: <http://modulo.com.br/index.jsp> Acesso em: 21 mar. 2005.

GRUPO SPISIS. **CDS/ISIS – Microisis**, 2000-2004**.** Disponível em <http://www.grupospisis.com.br/cdsisis/cdsisis.asp> Acesso em 21 set. 2005.

LIMA, A. O. R. de. Comentários sobre a lei Sarbanes-Oxley, **NF Online**, abr. 2004. Disponível em: <http://www.noticiasforenses.com.br/artigos/nf189/online/alex-lima-189.htm> Acesso em 23 nov. 2005.

LOBO, M. de F. D.; BARCELLOS, S. de O. Guias de fontes de informação: metodologia para geração e automação. **Ciência da Informação,** Brasília, v. 21, n. 1, p. 75-81, jan./abr. 1992.

MACHADO, C. de S. **51 questões mais freqüentes formuladas sobre a BS 7799 e ISO 17799**, set. 2004. Disponível em: <http://www.cddigital.com.br/iso/faq.htm> Acesso em 23 mar. 2005.

MALHOTRA, N. **Pesquisa de marketing:** uma orientação aplicada. 3 ed. Porto Alegre: Bookman, 2001. 720 p.

MANUAL. In: FERREIRA, A. B. de H. **Minidicionário da língua portuguesa.** 3. ed. Rio de Janeiro: Nova Fronteira, 1993. p. 350.

MANUAL. In: HOUAISS, A.; VILLAR, M. de S. **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Objetiva, 2001. p. 1842.

MÓDULO SECURITY. **Olhar para o próprio umbigo.** Disponível em: <http://www.modulo.com.br/empresa3/noticias/ITWEB-311002.htm> Acesso em: 23 ago. 2005.

OLIVEIRA, S. de. **As tríplices da segurança da informação,** 14 mar. 2005. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=429&pagecounter=0&idiom=0> Acesso em: 30 mar. 2005.

PLACER, X. **Técnica do serviço de referência.** Ed. Preliminar. Rio de Janeiro: Associação brasileira dos bibliotecários, 1968. 120 p.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003. 156 p.
STAIR, R. H. **Princípios de sistemas de informação:** uma abordagem gerencial. 4. ed. Rio de Janeiro: LTC, 2002. 496 p.

SYMANTEC. **O padrão de segurança global emergente: ISO 17799,** 02 abr. 2002. Disponível em: <http://www.symantec.com.br/region/br/enterprisesecurity/content/framework/BR_1261.html> Acesso em: 21 mar. 2005.

TORRES, E. F.; MAZZONI, A. A. Conteúdos digitais multimídia: o foco na usabilidade e acessibilidade. **Ciência da Informação,** Brasília, v. 33, n. 2, p. 152-160, maio/ago. 2004.

UEMURA, C. N. **A importância da segurança da informação,** 28 mar. 2005. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=432&pagecounter=0&idiom=0> Acesso em: 30 mar. 2005.

WEINBERG, G. M. **Consultoria:** o segredo do sucesso. São Paulo: McGraw-Hill, 1990. 259 p.

APÊNDICE 1 – ROTEIRO PARA ENTREVISTA EM PROFUNDIDADE

ROTEIRO PARA ENTREVISTA EM PROFUNDIDADE

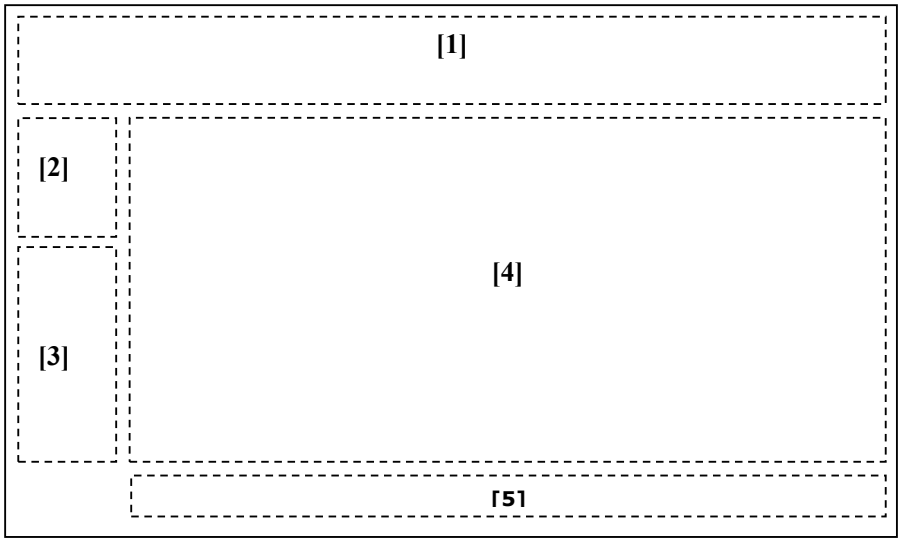
1. O que vem a sua mente quando você pensa num manual?
2. Pense nas vezes em que comprou algum produto que viesse com um manual de instruções, você os leu?
    2.1. Quando (na hora da compra ou depois quando surgiu alguma dúvida)?
    2.2. Por que leu, ou por que não leu?
3. Que característica você acha ruim nos manuais em geral?
4. O que você mudaria nos manuais se fosse o fabricante do produto?
5. O que vem a sua mente quando pensa em segurança de informações?
    5.1. Já pesquisou sobre o assunto?
        a. Encontrou o que queria?
        b. Algum tipo de informação nessa área é rara, difícil de ser encontrada?
    5.2. Quais as dificuldades encontradas?
6. O que entende por um SGSI*?
7. Alguma vez já participou do processo de implantação de um SGSI*?
    7.1. Havia uma metodologia ou um planejamento claro para isso?
    7.2. Quais as dificuldades encontradas?
    7.3. O que você fez que não faria numa próxima oportunidade?
    7.4. O que você não fez e que faria numa próxima oportunidade?
8. Se você fosse designado para a tarefa da construção de um manual que auxilie o planejamento estratégico da implantação de um SGSI*, ou seja, sem as especificidades técnicas próprias da informática, quais seriam as informações que você colocaria nele?
9. O que, na sua opinião, você acha que gerentes/administradores interessados na implantação de um SGSI* em suas empresas precisam saber sobre SGSI*?
10. De que maneira você o publicaria (especifique o meio, o "visual", etc.)?
11. Imagine que você esteja desenvolvendo esse manual para um público específico: administradores interessados na implantação de um SGSI* em suas empresas. Que critérios você consideraria importantes serem considerados para que esse manual desperte o interesse e chame a atenção dessas pessoas?
12. Na sua opinião, quais seriam as vantagens e desvantagens da criação desse manual?

---

* SGSI – Sistema de Gestão de Segurança da Informação

APÊNDICE 2 – ESBOÇO DO LEIAUTE DO PROTÓTIPO DE GUIA

ESBOÇO DO LEIAUTE DO PROTÓTIPO DE GUIA



[1] Nome do Guia:

a) será fixo;
b) nome: *GeSec – Guia de Fontes de Informação para Implantação de um Sistema de Gestão de Segurança da Informação (SGSI)*

[2] *Links* Sobre o Guia:

a) serão fixos;
b) lista dos *links* e ao que remetem:
   - *introdução ao tema: texto sobre segurança da informação;*
   - *como usar: instruções sobre como usar o Guia;*
   - *objetivo: apresenta o objetivo para o qual o Guia foi criado;*
   - *metodologia: explica sucintamente como o Guia foi montado;*
   - *contato: oferece um meio para contato do usuário com o produtor do Guia;*
   - *glossário: palavras do Guia com seus significados.*

[3] Links das Etapas para Implantação de um SGSI:

a) serão fixos;
b) cada link remeterá a um breve texto explicativo sobre a aplicação da etapa a que corresponde;
c) lista dos *links* e o conteúdo de suas páginas:
   - *compra da norma: quais existem;*
   - *treinamento: quando e como fazer;*
   - *equipe interna: como organizar;*
   - *consultoria: como trabalham e como escolher;*
   - *escopo do SGSI: delimitação do sistema;*
   - *avaliação de risco: como fazer;*
   - *política de segurança: como estruturar;*
   - *documentos de apoio: como montar;*
   - *implementação do SGSI: como fazer*
   - *auditoria interna: o que envolve;*
   - *certificação: como conseguir;*
   - *melhorias e controles: porque dar continuidade.*

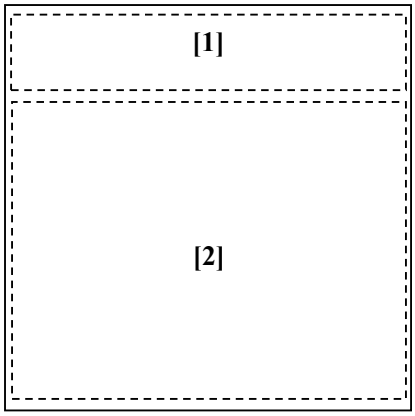
[4] Texto:

a) será variável de acordo com o conteúdo do link que estiver ativo;
b) quando for relacionado a algum link das etapas de implantação de um SGSI, haverá no texto um outro link remetendo a tela de fontes de informação.

[5] Rodapé:

a) conterá a data de atualização, melhor configuração para visualização e detalhes da produção.

» Tela de Fontes de Informação



[1] Identificação:

a) será fixa;
b) conterá o nome "GeSec" e o número ordinal e nome da etapa a que corresponde.

[2] Fontes de Informação:

a) conterá a lista de fontes de informação relacionadas à etapa correspondente:
   - *normas: onde comprar;*
   - *treinamento: quem faz;*
   - *equipe interna: referências sobre como gerenciar uma equipe;*
   - *consultoria: quais são algumas delas;*
   - *escopo do SGSI: referências que apresentam como fazer;*
   - *avaliação de risco: referências que ensinam como fazer;*
   - *política de segurança: referências sobre como estruturar*
   - *documentos de apoio: referências que mostram como estruturar;*
   - *implementação do SGSI: referências que ensinam como fazer;*
   - *auditoria interna: referências que especificam os aspectos envolvidos;*
   - *certificação: quem faz;*
   - *melhorias e controles: referências que garantem a atualização no assunto.*
b) as fontes serão identificadas com um nome;
c) será oferecido um link direto para a fonte;
d) será dada uma breve descrição da fonte;
e) o restante do conteúdo de cada referência é relativo, podendo conter: autor, datas, observações, entre outros;
f) no canto inferior direito da tela haverá *links* fixos que remetem às listas fontes das demais etapas da implantação do SGSI.

APÊNDICE 3 – QUESTIONÁRIO DE AVALIAÇÃO DO PROTÓTIPO

QUESTIONÁRIO DE AVALIAÇÃO

Este questionário tem como finalidade avaliar o **protótipo de um Guia de Fontes de Informação para Implantação de um SGSI** (Sistema de Gestão de Segurança da Informação). Como se trata de um protótipo, este produto **NÃO** é 100% completo em seu conteúdo. Assim sendo, o objetivo principal deste questionário é levantar informações que possam contribuir para melhorar e/ou corrigir aspectos necessários no Guia para dar continuidade à sua construção.

O Guia encontra-se disponível no endereço: **http://geocities.yahoo.com.br/carolrogal**

>> Marque sempre APENAS UMA ALTERNATIVA para cada tópico!

1. Quanto à aparência do Guia (seu aspecto visual)

» Considerando o TÍTULO DO GUIA (parte superior):

a) O estilo de letra é:	b) O tamanho das letras é:	c) A cor das letras é:
( ) adequado	( ) adequado	( ) adequado
( ) inadequado	( ) inadequado	( ) inadequado
( ) prefiro não opinar	( ) prefiro não opinar	( ) prefiro não opinar

» Considerando os *LINKS* (situados na coluna esquerda)

a) O estilo de letra é:	b) O tamanho das letras é:	c) A cor das letras é:
( ) adequado	( ) adequado	( ) adequado
( ) inadequado	( ) inadequado	( ) inadequado
( ) prefiro não opinar	( ) prefiro não opinar	( ) prefiro não opinar

» Considerando o CONTEÚDO CENTRAL das páginas (texto principal)

a) O estilo de letra é:	b) O tamanho das letras é:	c) A cor das letras é:
( ) adequado	( ) adequado	( ) adequado
( ) inadequado	( ) inadequado	( ) inadequado
( ) prefiro não opinar	( ) prefiro não opinar	( ) prefiro não opinar

» Considerando a janelinha de FONTES DE INFORMAÇÃO (para ver essa janela entre numa das etapas do guia e clique em "para conhecer fontes de informação relacionadas ao tema: **clique aqui!**")

a) O estilo de letra é:	b) O tamanho das letras é:	c) A cor das letras é:
( ) adequado	( ) adequado	( ) adequado
( ) inadequado	( ) inadequado	( ) inadequado
( ) prefiro não opinar	( ) prefiro não opinar	( ) prefiro não opinar

» Considerando o Guia num aspecto GERAL (todas as suas páginas)

a) As cores de fundo são:
( ) agradáveis
( ) não agradáveis
( ) prefiro não opinar

b) A maneira como a informação foi organizada (com o título na parte superior, os *links* à esquerda e o texto principal centrado) é:
( ) totalmente adequada
( ) adequada
( ) inadequada
( ) totalmente inadequada
( ) prefiro não opinar

» Escreva suas críticas ou elogios quanto à aparência geral do Guia:
_____
_____
_____
_____

2. Quanto à usabilidade (facilidade de uso) do Guia:

a) O uso do guia permite a auto-aprendizagem, isto é, você consegue entendê-lo sozinho, sem precisar de auxílio?
( ) sim
( ) não
( ) prefiro não opinar

Caso tenha marcado não, qual(is) foi(ram) a(s) dificuldade(s) encontrada(s)?
_____
_____
_____
_____

b) O guia está livre de erros?
( ) sim
( ) não
( ) prefiro não opinar

Caso tenha marcado não, que erro(s) foi(ram) encontrado(s)?
_____
_____
_____
_____

» Escreva suas críticas ou elogios quanto à usabilidade geral do Guia:

_____
_____
_____
_____

3. Quanto ao conteúdo do Guia:

a) Os textos, de modo geral, estão escritos de forma clara, de fácil compreensão?
( ) sim
( ) não
( ) prefiro não opinar

Caso tenha marcado não, especifique em qual(is) parte(s) ele não está claro.

_____
_____
_____
_____

b) O Guia cobriu toda a informação que você considera importante?
( ) sim
( ) não
( ) prefiro não opinar

Caso tenha marcado não, que tipo de informação(ões) – na sua opinião – está(ão) faltando?

_____
_____
_____
_____

c) As informações contidas no Guia facilitaram a percepção da Segurança da Informação no contexto da empresa onde trabalha, isto é, você percebeu aspectos que tem sido ou que faltam ser implementados na sua organização através do Guia?
( ) sim
( ) não
( ) prefiro não opinar

d) As informações contidas no Guia podem de alguma forma auxiliá-lo na tomada de decisão em relação aos aspectos que a Segurança da Informação envolve na sua empresa?
( ) sim
( ) não
( ) prefiro não opinar

» Escreva suas críticas, sugestões ou elogios quanto ao conteúdo geral do Guia:

_____
_____
_____
_____
_____

APÊNDICE 4 - FICHA DE LEVANTAMENTO DE FONTES VIRTUAIS

FICHA PARA FONTES VIRTUAIS

Endereço de acesso:_____

Endereço/bibliografia
( ) Endereço eletrônico: título, autor, instituição, endereço, ano da fonte.
( ) Livro: título, autor, edição, local, editora, ano, localização física.
( ) Periódico: título do artigo, autor, nome da revista, editora, volume, número, mês, ano.
_____
_____
_____

Periodicidade
A fonte é publicada de quanto em quanto tempo?_____

Certificação
( ) Não ( ) Sim, qual?_____

Acesso
Precisa de software específico para acessar? ( ) Não ( ) Sim, qual?_____

Taxas/assinaturas
Tem que pagar? ( ) Não ( ) Sim, quanto?_____

Precisão
A informação baseia-se no quê? ( ) Pesquisas ( ) Opinião pessoal
Passou por processo editorial ou de revisão? ( ) Não ( ) Sim

Resumo
Escrever um breve resumo no verso.

Estabilidade
Verificação da disponibilidade da fonte quando for publicada a edição "final" do guia.
( ) Não ( ) Sim

Etapa(s) a que se relaciona:
( ) Compra da Norma
( ) Equipe Interna
( ) Escopo SGSI
( ) Política de Segurança
( ) Implementação do SGSI
( ) Certificação
( ) Treinamento/Conscientização
( ) Consultoria
( ) Avaliação de Risco
( ) Documentos de Apoio
( ) Auditoria Interna
( ) Melhorias e Controles

APÊNDICE 5 – FICHA PARA SELEÇÃO DE CONSULTORIAS

FICHA PARA LEVANTAMENTO DE CONSULTORIAS

Endereço de acesso:_____

Critérios de SÊMOLA (2003, p. 68)

Posicionamento e perfil de Consultoria e Integradora de Ferramentas.
( ) Sim ( ) Não

Notória especialização em Segurança da Informação.
( ) Sim ( ) Não

Especificidade em Segurança da Informação.
( ) Sim ( ) Não

Equipe técnica multiespecialista.
( ) Sim ( ) Não

Ação local com visão global.
( ) Sim ( ) Não

Estrutura de execução de projetos capaz de viabilizar ações simultâneas em paralelo.
( ) Sim ( ) Não

Metodologia para dimensionamento de solução que considere fundamentalmente as características e desafios de negócio.
( ) Sim ( ) Não

Metodologia específica para execução de projetos de segurança da informação.
( ) Sim ( ) Não

Metodologias em conformidade com as normas internacionais BS7799 e ISO17799.
( ) Sim ( ) Não

Presença geográfica proporcional ou capaz de atender às características da empresa.
( ) Sim ( ) Não

Ponto de presença no exterior, viabilizando a absorção de experiências, inovações e tendências, e facilitação de parcerias e contatos técnicos.
( ) Sim ( ) Não

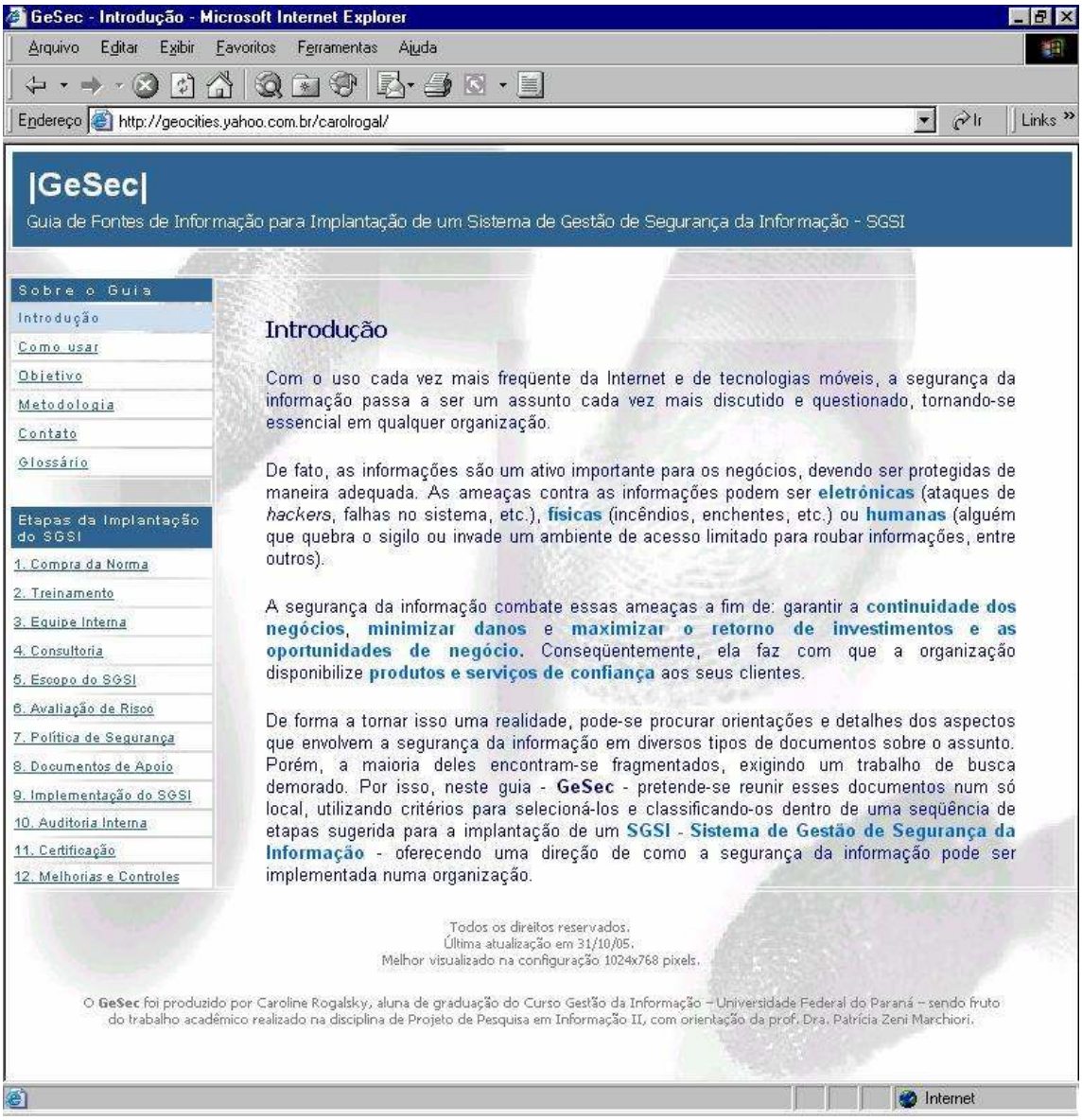
Comprovada experiência em projetos corporativos complexos.
( ) Sim ( ) Não

Resumo
Escrever um breve resumo no verso.

Estabilidade
Verificação da disponibilidade do endereço eletrônico quando for publicada a edição "final" do guia.
( ) Sim ( ) Não

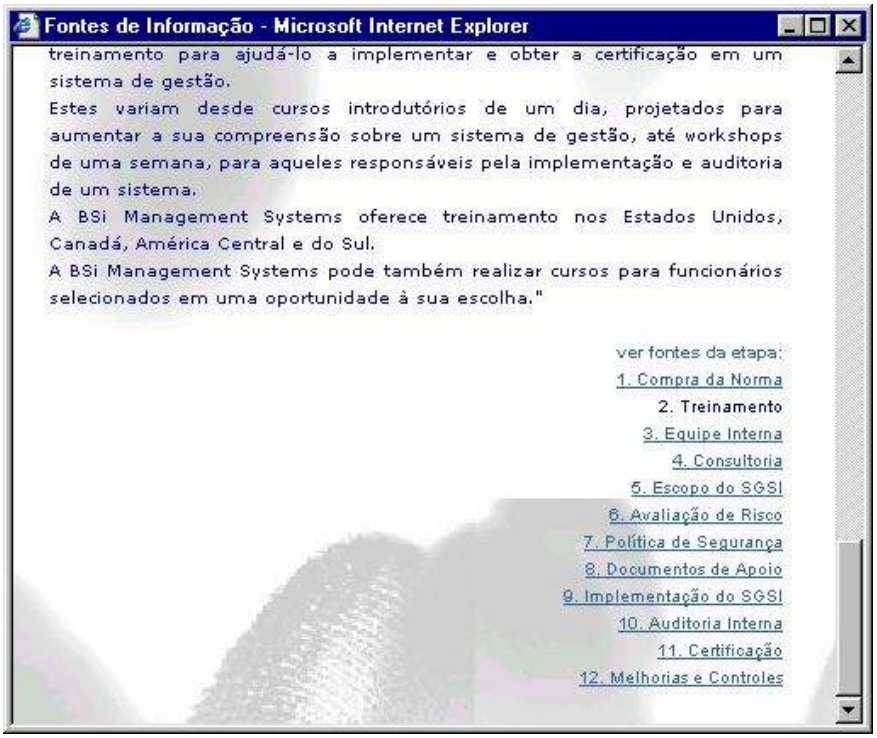
APÊNDICE 6 – PROTÓTIPO DO GUIA

PÁGINA INICIAL DO PROTÓTIPO DO GUIA



PÁGINA DE UMA DAS ETAPAS DE IMPLANTAÇÃO DE UM SGSI

JANELA DAS FONTES DE INFORMAÇÃO RELATIVAS A CADA ETAPA DE IMPLANTAÇÃO DE UM SGSI*



* As janelas estão em formato reduzido.