FACULDADES IBMEC
PROGRAMA DE PÓS-GRADUAÇÃO E PESQUISA EM
ADMINISTRAÇÃO E ECONOMIA

DISSERTAÇÃO DE MESTRADO
PROFISSIONALIZANTE EM ADMINISTRAÇÃO

PROPOSTA DE METODOLOGIA PARA A ELABORAÇÃO DE UM PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

RAMIRO FERNANDES RODRIGUES FILHO

ORIENTADOR: PROF. DR. VALTER MORENO JR.

RIO DE JANEIRO, ABRIL DE 2005

DEDICATÓRIA

Dedico este trabalho a meus pais Ramiro e Iara, pela dedicação incondicional e princípios passados.

Dedico também a minha mulher. Mais que companheira, um exemplo a ser admirado e seguido.

AGRADECIMENTOS

A Deus que me deu saúde e perseverança.

A meus pais que, além dos valores de justiça e sensatez, tanto se empenharam em deixar-me a melhor das heranças : a educação.

A minha mulher, pelo incentivo em começar, pela presença no continuar, e pela visão de onde chegar.

Ao professor Valter Moreno Jr. que acreditou, orientou e se empenhou em ajudar a construir esta dissertação.

A todos os colegas de trabalho, clientes e pesquisadores, que de alguma forma contribuíram para consolidar as experiências e conhecimentos demonstrados neste trabalho.

RESUMO

No atual cenário corporativo mundial, muitas organizações têm buscado implantar sistemas de informação adequados como uma forma de obter um diferencial competitivo. Como parte das melhorias de seus sistemas, muitas organizações avançaram seriamente na implementação de planejamentos eficientes na segurança da informação e seus principais aspectos – a confidencialidade, a integridade e a disponibilidade das informações, por compreenderem que, desta forma, obteriam o nível de qualidade no uso das informações capaz de agregar real valor aos seus negócios. No entanto, ainda não há consenso entre os responsáveis pela gestão dos sistemas da informação e de sua segurança sobre a adoção de um modelo consistente e coerente para a estruturação de um planejamento de ações eficaz, tendo em vista as características de suas respectivas organizações. Este trabalho propõe um método para a estruturação do planejamento de segurança da informação para uma empresa contemplando e respeitando as particularidades de sua estrutura organizacional e seus objetivos estratégicos.

ABSTRACT

Lately, in the corporate world scenario, many companies have tried to implement adequate information systems as a way of obtaining a competitive differential. As part of the improvement in their systems, many organizations advanced considerably in the implementation of efficient management concerning information security and its main aspects – confidentiality, integrity and availability of information; since they understood that, through this, they would obtain a level of quality in the use of information capable of aggregating real value to their business. However, there is still no consensus, among those responsible for managing the information systems and its security, about the adoption of a consistent and coherent methodology to structure a plan of efficient actions, bearing in mind the characteristics of their respective organizations. This paper proposes a framework to structure a plan regarding information security for a company, considering and respecting the particularities of its organizational structure and strategic objectives.

SUMÁRIO

LISTA DE TABELAS, GRÁFICOS E FIGURAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

BS	British Standard
BSI	British Standard Institute
CCSC	Commercial Computer Security Centre
CID	Conjunto de conceitos para análise de sensibilidade – Confidencialidade, Integridade e, Disponibilidade.
GAS	Goal Attainment Scaling
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicators
MCDM	Multiple Criteria Decision Making
N/A	Não se aplica
NBR ISO/IEC	Normas Brasileiras - International Standardization Organization/ International Engineering Consortium
PDCA	Modelo de gestão implementado originalmente na ISO 9000 – *Plan, Do, Check* e *Act*.
PDSI	Plano Diretor de Segurança da Informação
PN	Processo(s) de negócio
RFC	Request for Comment
SGSI	Sistema de Gestão de Segurança da Informação.
SI	Segurança da Informação
UT	Urgência e Tendência

1. INTRODUÇÃO

A sociedade observa uma evolução na valorização da informação reconhecendo-a como um ativo intangível de grande valor para as corporações (Leal, 2000). Nestas, o grande desafio é fazer com que seus sistemas de informação sejam eficientes insumos, capazes de dar suporte, de forma eficaz e eficiente, à tomada de decisões. Para seus executivos, a informação passou a ser um recurso-chave, mas poucos esforços parecem ser feitos para averiguar o que realmente é necessário e como organizá-las para atender às suas necessidades específicas. Assim, os produtores de informação ganharam muito mais espaço nas corporações do que aqueles que realmente necessitam da informação, pois, somente estes (produtores de informação) poderiam discernir e organizar informações que eram úteis e que poderiam se traduzir em ações eficazes (DRUCKER, p.103). Em outras palavras, reconhece-se a necessidade de transformação das informações em poderosas ferramentas a serviço dos interesses de gestão estratégica da organização.

Com o entendimento destas responsabilidades, as corporações vêm exigindo de seus executivos uma combinação de novos conhecimentos, habilidades e maior velocidade na tomada de decisões. A tendência é confirmada por FARAH (1999, p. 4) quando diz:

> "A evolução tecnológica tem sido intensificada causando uma obsolescência crescente sobre os meios de produção e processos, onde a inovação e a atualização têm sido consideradas básicas para as empresas superarem os padrões anteriores de conhecimento, tecnologia, equipamentos e de gestão. [...] Esta nova forma de organizar o trabalho e a produção, passa a exigir mão-de-obra capacitada e com maior nível de escolaridade formal, com maior apropriação de tecnologia e conhecimento, capacidade de decisão e responsabilidade."

Por sua vez, exigências de velocidade e disponibilidade de operações trazem vulnerabilidades de segurança e ameaças às informações críticas e vitais para a corporação. Segundo a pesquisa realizada pela Ernst & Young, onde 459 diretores de TI e executivos de diversos países foram entrevistados, a velocidade de mudanças e a crescente sofisticação das empresas, foram

apontadas como os principais desafios relacionados à segurança da informação, com 70% dos votos (ERNST & YOUNG, 2002, p.10).

Percebeu-se nos últimos anos, o início de um processo de formação de profissionais especializados na proteção das informações estratégicas das corporações. A estes gestores da segurança da informação (SI), também reconhecidos como *Security Officers*, caberia a responsabilidade de conciliar os interesses dispostos no plano estratégico de negócio de sua organização com a gestão e manutenção dos principais aspectos da segurança da informação.

Sinteticamente, a área de Segurança da Informação procura preservar três aspectos básicos da informação: a confidencialidade, a integridade e a disponibilidade (NBR ISO/IEC 17799:2001, p. 4), descritos no capítulo 1.3.2 deste trabalho.

O *Security Officer* é definido, na RFC[1] 2828, como "a pessoa responsável pela aplicação ou administração da política de segurança aplicável ao sistema" (RFC 2828, 2000, tradução nossa). MARINHO (2001, p. 1) detalha as atribuições do *security officer* da seguinte forma:

> *"Security Officer* é o principal responsável pela gestão da segurança da informação nas organizações. Suas atribuições compreendem, dentre outras funções:
> - Organizar o *Security Office*[2] e a infra-estrutura organizacional responsável pelo tratamento da segurança;
> - Planejar os investimentos para a Segurança da Informação;
> - Definir índices e indicadores para análise de retorno do investimento;
> - Montar, orientar e coordenar a equipe e consultoria terceirizada;
> - Definir, elaborar, divulgar, treinar, implementar e administrar juntamente com sua equipe o Plano estratégico de Segurança".

Profissionais encarregados destas responsabilidades têm encontrado dificuldade para apoiar-se em referências bibliográficas, visto que somente em 2000, a literatura internacional e nacional começou a esboçar matérias mais objetivas sobre o tema, principalmente a partir da publicação da norma *British*

---

[1] As *Request for Comment* (RFC) são relatórios resultantes de investigações e experimentos que contém especificações técnicas para serem comentadas pelos leitores interessados no desenvolvimento da Internet.

Standard 7799 que se tornou um marco inicial no fomento de alguns trabalhos em sítios e revistas especializadas sobre o planejamento de atividades na área. Entretanto, as publicações literárias que começaram a surgir, a partir de então, ainda apresentam resultados dispersos, o que não garante ao gestor da segurança da informação um apoio consistente e um referencial para a elaboração de seu plano diretor de segurança da informação.

1.1. O Mercado de Segurança da Informação

Alguns ramos de atividades, como o bancário e de serviços, já demonstram reconhecer a relevância da informação para seus negócios e a conseqüente necessidade de protegê-la (GOMES, 2005). Segundo a 9ª. Pesquisa Módulo de Segurança da Informação, onde 682 profissionais especializados ligados às áreas de tecnologia e segurança da informação foram entrevistados (MÓDULO, 2003, p. 14): "51% dos entrevistados percebem nos executivos de suas empresas a consideração da Segurança da Informação como *fundamental* para a integridade e continuidade de seus negócios, sendo que para 21% é fator *vital* e para 16% é *crítica*".

Para se ter uma noção da relevância mercadológica da segurança da informação, conforme um estudo do *INSTITUTO DE INTELIGÊNCIA DE MERCADO E CONSULTORIA DE TI E TELECOMUNICAÇÕES - IDC*, divulgado através da revista eletrônica Techworld.com e traduzida pela Computerworld (2004): "os gastos com segurança deverão chegar a US$ 48 bilhões em todo o mundo, apenas 4,8% de todos os gastos com TI. O estudo revela que, até 2007, as empresas deverão gastar cerca de 7% de seu orçamento com a segurança de seus dados e operações".

Portanto, a estimativa é de que, até 2007, os orçamentos da área de segurança da informação irão somar US$ 70 bilhões, dentro de um orçamento mundial dos gastos com TI estimado em US$ 1 trilhão.

---

[2] Segundo BARBOSA (2002, pág.1), *Security Office* é uma estrutura organizacional dimensionada para a coordenação, execução e manutenção de atividades relacionadas à segurança da informação.

1.2. Objetivos

O objetivo principal deste trabalho é descrever um modelo heurístico para a implantação de um plano plurianual de segurança da informação, com base na BS7799 e na literatura disponível, onde são definidos aspectos de priorização, esforço, custeio e recursos na execução de projetos ligados à segurança da informação. Apoiado nas melhores práticas internacionalmente reconhecidas, este planejamento deve fornecer meios para identificar a situação atual e pretendida do nível de segurança da organização, a fim de tornarem-se insumos nas decisões sobre investimentos na área de segurança da informação, em conformidade com as estratégias de suas organizações.

O público-alvo deste trabalho são os profissionais responsáveis pela gestão da segurança da informação (SI) dentro de corporações empresariais brasileiras. Não obstante, para o melhor entendimento deste trabalho, é necessário apenas conhecimento genérico sobre a área de SI, não sendo pré-requisito aprofundado conhecimento tecnológico sobre a matéria.

2. REVISÃO DA LITERATURA

Hoje, já se percebe no mercado corporativo, uma quantidade considerável de eventos e congressos que fomentam a interação entre os profissionais gestores da segurança da informação. No entanto, ainda é bastante limitada a literatura disponível sobre o tema. Isto pode se dever não somente ao recente interesse por este tópico, mas também pela aparente resistência das empresas em tornar público dados sobre seu grau de maturidade em segurança da informação, conforme observado na pesquisa realizada para este trabalho.

Assim, mesmo com uma situação progressiva, mas ainda inicial, das iniciativas de segurança da informação dentro das corporações, os responsáveis pela gestão da SI têm ainda dificuldades para encontrar um referencial metodológico no momento de estruturar suas ações e prioridades, e de localizar respostas para questões como: *O que devo fazer primeiro? Implementar uma política de segurança ou uma análise de riscos? Que áreas críticas devem ser priorizadas? Devo fazer uma classificação da informação? Em toda a empresa ou nos processos críticos? Que recursos humanos e financeiros serão necessários para isso?*

À luz deste cenário, esta revisão da literatura procurou identificar os trabalhos científicos que se paralelizam com os objetivos deste trabalho, traçando uma visão comparativa que expõe as lacunas de aprofundamento a serem ainda preenchidas, além de obras de mercado de reconhecida importância para os gestores de segurança da informação.

Para as próximas seções são apresentados tópicos que iniciam com uma descrição do consenso literário dos conceitos de SI. Após e devido a sua relevância neste contexto, é dedicado um tópico à norma BS7799, sendo descritos seu histórico e objetivos. Em seguida é discutida a importância de realizar o planejamento de segurança da informação, as atuais metodologias identificadas e suas carências, o que está sendo feito hoje, quais os benefícios de pesquisar esta área, problemas identificados e diferenças com este trabalho. Por fim, as conclusões do autor sobre toda a literatura utilizada.

2.1. O Conceito de Segurança da Informação

Segundo a NBR ISO/IEC 17799:1 (ABNT, p. 2):

> "a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. 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".

Cabe reforçar o entendimento de que a informação existe em diversas formas. Embora estejamos em uma era onde é crescente o uso e o armazenamento da informação eletrônica, existe igual validade (e vulnerabilidades) na informação impressa, falada etc. (Globo OnLine, 2003). Independentemente da forma, é importante perceber que informações devem se adequar para o correto uso e armazenamento perante os aspectos de confidencialidade, integridade e disponibilidade (ABNT, p. 2).

É indiscutível a crescente dependência das organizações sobre seus sistemas de informação. Sabe-se também que a infra-estrutura tecnológica que suporta estes sistemas é constantemente testada por cada vez mais sofisticadas ameaças, como vírus, intrusões, espionagem, tentativas de indisponibilidade dos serviços etc. onde, apenas no primeiro no semestre do ano de 2004, foram detectados 11.650 novos vírus, quase o dobro do segundo semestre de 2003 (6.430 novos vírus) e sete vezes mais do que os 1.650 identificados no primeiro semestre do ano de 2003 (ComputerWorld, 2004). Diante destas crescentes ameaças à segurança das redes corporativas, somente o mercado de softwares antivírus projetou um crescimento de 21% nas vendas em 2003, que atingiram US$ 2,7 bilhões (IDG Now!, 2004). O balanço resultante desta crescente dependência de informações e das ameaças a que estas estão sujeitas, remonta a um quadro de delicada dedicação necessária às organizações no esforço de se manterem funcionais e competitivas.

2.1.1. Conceitos Básicos de Segurança da Informação

A fim de promover o bom entendimento dos argumentos apresentados ao longo do trabalho, são descritos a seguir, alguns dos principais conceitos da segurança da informação.

- Ativo – Tudo o que manipula direta ou indiretamente a informação, inclusive ela própria. Equipamentos, sistemas, informações em qualquer mídia e pessoas são exemplos de ativos da segurança da informação;
- Ameaça - Agente ou condição capaz de desencadear um ou uma série de incidentes;
- Incidente - Efetiva concretização de uma ameaça que ocasione perda ou dano ao ativo, causando sua indisponibilidade e/ou comprometimento do processo de negócio;
- Vulnerabilidade - Grau de exposição que uma informação ou processo de negócio possui em relação a uma ou várias ameaças;
- Risco – Corresponde à probabilidade de ameaças explorarem vulnerabilidades pelos possíveis impactos causados;
- Impacto – Análise do dano (ou conseqüência) em um ou mais processos de negócio de uma corporação, caso haja quebra de um dos aspectos de segurança;
- Autenticação – Propriedade que visa reconhecer e validar o processo de identificação de acesso de uma entidade em um processo de comunicação;
- Autenticidade – Propriedade que garante que as entidades participantes de um processo de comunicação são exatamente aquelas que dizem ser;
- Legalidade - Propriedade da informação que possui conformidade com preceitos de obediência a valores legais vigentes dentro de um processo de comunicação.

2.1.2. Análise de Sensibilidade

Os conceitos básicos da segurança da informação, confidencialidade, integridade e disponibilidade, identificados pela NBR/ISO 17799 (ABNT, p. 2) servem de base para o conjunto de propriedades que identificam o grau de sensibilidade à quebra de seus aspectos. São eles: confidencialidade – propriedade que garante que as informações somente estão acessíveis às entidades (pessoas, processos ou sistemas) autorizadas para tal ; integridade –

propriedade que assegura que a informação, ou seus recursos, não foi modificada. Cabe reforçar o entendimento que este conceito não se baseia em garantir a veracidade da informação mas sim, que esta será resgatada da mesma forma como foi gerada; e, disponibilidade – propriedade que garante que as entidades requerentes obtenham acesso à informação sempre que requisitado.

2.1.3. Análise de Priorização

Já, os conceitos de urgência e tendência, fornecem a base para o conjunto de propriedades que identificam as necessidades de priorização e quais processos necessitam de respostas com maior velocidade. Podem-se descrever seus conceitos como: Urgência – é a necessidade de rapidez na implementação de ações corretivas caso haja a quebra de um dos aspectos de segurança em um ou mais processos de negócio de uma corporação; Tendência – é a percepção prevista do nível de vulnerabilidade de um ou mais processos de negócio ao longo do tempo, caso não sejam melhorados os atuais níveis de segurança das informações.

2.2. A História da BS7799

Em 1987 o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, denominado *Commercial Computer Security Centre* (CCSC). Dentre as atribuições deste centro havia a tarefa de se criar um documento técnico que fixasse padrões reguladores visando garantir a segurança da informação através da criação de critérios para a avaliação. Outro objetivo do CCSC era a criação de um conjunto metódico e sistemático de disposições legais relativas à segurança para os usuários das informações. Assim, em 1989, foi produzida e publicada a primeira versão do documento *PD0003 – Código para Gerenciamento da Segurança da informação* (Casanas e Machado, 2003).

Em 1995, esse documento foi revisado pelo *British Standard Institute* (BSI) e publicado com o nome de BS7799:1995. Como anteriormente ocorrido com outras normas originadas do BSI como, por exemplo, a BS5750 homologada como ISO 9000 (qualidade) e, a BS7550 homologada como ISO 14000 (meio ambiente), em 1996, essa norma foi igualmente proposta à

International Organization for Standardization (ISO) para homologação mas foi rejeitada (Hefferan, 2000). A International Organization for Standardization é uma rede de institutos nacionais de padrões presente em 148 países, com sede em Genebra, Suíça. A ISO ocupa uma posição especial entre os setores públicos e confidenciais, pois age como uma organização que procura consenso nas soluções de exigências de mercado e necessidades da sociedade, tais como as relações de consumidores e usuários. Não obstante, a ISO é adotada como ferramenta de padronização de qualidade na produção e serviços de diversos setores econômicos e sociais.

Em novembro de 1997, foi criada uma segunda parte desse documento para consulta pública e avaliação. Em 1998, esse documento foi publicado com o título de BS7799-2:1998 e, depois de revisado, foi publicado em conjunto com sua primeira parte em abril de 1999 como BS7799:1999 (Hefferan, 2000).

A parte 1 desse documento foi levada à ISO e proposta para homologação pelo mecanismo denominado "*fast track*" a fim de se obter um trâmite rápido para sua homologação, visto que, normalmente, uma norma leva cerca de cinco anos para ser avaliada e homologada pela ISO. Em outubro de 2000, esta parte da norma, foi novamente apresentada ao comitê da ISO e, desta vez, aprovada pelo instituto, sendo então, homologada sob a denominação ISO/IEC 17799:2000 em 1º. de dezembro de 2000 (Casanas e Machado, 2003).

Em agosto de 2001 e, com a homologação da ISO, o Brasil também adotou a norma como seu padrão para um código de prática para gestão da segurança da informação, através da Associação Brasileira de Normas Técnicas (ABNT), sob a denominação NBR ISO/IEC 17799.

Atualmente, o comitê BDD/2 do *British Standards Institution - Delivering Information Solutions to Customers* (BSI-DISC) está preparando a parte 2 da BS7799 para apresentação à ISO para homologação.

2.2.1. Objetivos da Norma

A parte 1 da BS7799 (BS7799-1) fornece recomendações para a gestão da segurança da informação e é composta de 10 domínios principais, também

chamados de *controles*[3] de 1º. nível, que aglutinam 36 controles de 2º. nível. Sua estrutura de controles é exemplificada na figura 1.

Sua maior aplicação é para gestores responsáveis por implementar e manter um sistema de gestão da segurança da informação em suas organizações. Conforme dito por BASTOS (2002, p. 1):

> "A norma estabelece uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas da gestão da segurança, facilitando o *benchmark* dos processos e provendo confiança nos relacionamentos entre as organizações".

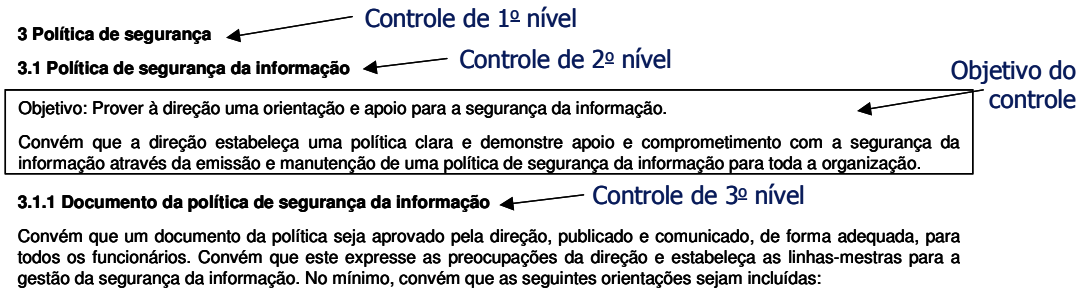

Figura 1: Estrutura de um controle da ISO 17799

A parte 2 da BS7799 (BS7799-2) tem por objetivo qualificar organizações que procuram nesta certificação diferenciais competitivos que comprovem o compromisso com a segurança das informações próprias ou custodiadas. A estrutura de segurança definida estabelece um Sistema de Gestão de Segurança da Informação (SGSI) que somado ao conjunto de controles sugeridos na primeira parte da norma serve de objeto para a certificação. Assim, empresas passam a conduzir as atividades de segurança da informação sob a orientação de uma base comum proposta pela norma, além de se preparar para o reconhecimento de conformidade aferido por órgãos credenciados. A busca por esta certificação, similar aos reflexos obtidos pela conquista da certificação de qualidade ISO 9000, parece procurar um diferencial de mercado que promova um fortalecimento nas relações com parceiros, clientes e fornecedores, através de uma demonstração pública de

[3] Segundo o dicionário AURÉLIO (1999), **controle** pode ser definido também como "*a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos, ou sobre produtos etc., para que tais atividades, ou produtos, não se desviem das normas preestabelecidas*". Neste trabalho, controles são entendidos como tópicos e sub-tópicos que definem o que deve ser feito para assegurar aquele item.

compromisso com a segurança das informações que possui e/ou custodia (Bastos, 2002).

Hoje e, conforme demonstrado na tabela 1, 1201 empresas no mundo possuem certificação BS7999 sendo três no Brasil, segundo informação atualizada em 8 de abril de 2005 no sítio oficial da *ISMS International User Group,* grupo internacional de usuários e estudiosos da parte 2 da BS7799, estabelecida pelo DTI (Departamento de Comércio e da Indústria do Reino Unido) em 1997 com o propósito de facilitar os meios de compartilhamento de experiências no uso destes padrões.

Japão	587	Suécia	7	Macedônia	1
UK	185	Áustria	5	Colômbia	1
Índia	91	Polônia	5	Egito	1
Alemanha	36	Suíca	5	Líbano	1
Coréia do sul	31	Islândia	4	Luxemburgo	1
Taiwan	45	Brasil	3	Macau	1
Italia	23	Grécia	3	Eslováquia	1
Holanda	18	México	3	Morocos	1
Hong Kong	17	Emirados Árabes	3	Quatar	1
EUA	16	Arábia Saudita	3	Eslovênia	1
Hungria	13	Espanha	3	República Tcheca	1
Finlândia	13	Bélgica	2	Lituânia	1
Singapora	11	Malásia	2	África do Sul	1
China	11	Argentina	2		
Irlanda	11	Dinamarca	2		
Austrália	11	Isle of man	2	Total Relativo[4]	1201
Noruega	9	Romênia	1	Total Absoluto	1190

Tabela 1: Número de empresas certificadas por país

Fonte: ISMS International User Group, 2005.

2.3. Planejamento da Segurança da Informação

Em 2002, um estudo conduzido pelo *Computer Security Institute* (CSI) e pelo *Federal Bureau of Investigation* (FBI) indicou que mais de 90% das

[4] O total absoluto representa o atual número de certificados. O total relativo reflete certificados que representam registros em multi-nações ou certificações duplas.

organizações pesquisadas tinham relatado incidentes com segurança de sistemas no ano de 2001, e estimavam perdas financeiras na ordem de US$ 455.848.000 (Power, 2002 *apud* El-Gayar e Fritz, 2004 p.1).

Para os próximos anos, são previstos incentivos e investimentos à segurança da informação, trazendo com isso a necessidade de planejamento para o melhor aproveitamento dos recursos a serem investidos (ComputerWorld, 2004).

Hoje e, conforme reforçado pela pesquisa realizada para este trabalho, observa-se uma série de iniciativas dispersas, como a utilização da BS7799, métodos de suporte a decisões, implementação de conceitos da metodologia *Information Technology Infrastructure Library* (ITIL), ou técnicas de análise de riscos. Deve-se avaliar portanto, o desenvolvimento de procedimentos que apõem-se a um planejamento mais amplo e que constituam um padrão que atenda a empresas de diferentes ramos.

Esta escassa referência de padrões para a elaboração de planejamento de atividades da área de SI parece permitir aos profissionais que as realizam, a adaptação de ações, decisões e procedimentos à perigosa conveniência de metodologias que lhes sejam de seu maior domínio. Observa-se, porém, que a falta de uma metodologia aceita e fundamentada científica e mercadologicamente cria problemas para os profissionais da área, quando precisam justificar suas solicitações de recursos para a execução de projetos em segurança da informação.

2.4. Metodologias de Segurança da Informação

Em um dos raros livros sobre o assunto publicados no Brasil, *Gestão da Segurança da Informação* de Sêmola (2003) procura apresentar uma visão estratégica sobre a segurança da informação, desde a conceituação básica do valor da informação como ativo intangível patrimonial, aos aspectos básicos da segurança – confidencialidade, integridade e disponibilidade, como um diferencial competitivo para as empresas, dentro de seus mercados de atuação. Os conceitos de riscos, ameaças, vulnerabilidades, medidas e impactos também são descritos. O autor apoiou-se em sua experiência de consultor de produtos e soluções na área da SI para a elaboração de sua obra. O livro se caracteriza

pelo forte direcionamento conceitual. Sua leitura torna-se, assim, de grande valia para profissionais iniciantes que necessitam de referencial conceitual na visão de gestão da segurança da informação.

Em seu trabalho, Sêmola dedica um capítulo à elaboração do que chama somente de “Plano Diretor de Segurança”. Nele, é sugerida uma metodologia baseada fortemente na análise de impactos: *Confidencialidade – Integridade – Disponibilidade – Autenticidade – Legalidade (CIDAL)* e, na análise de prioridade: *Gravidade – Urgência – Tendência (GUT)*, além do estudo de perímetros, e da estruturação das atividades. Descreve ainda, a necessidade de mapeamento dos processos de negócio a serem objetos do plano e do relacionamento entre estes e seus itens de infra-estrutura (física, tecnológica e humana), além de esclarecer o modelo proposto pela norma BS7799, originada no modelo *Plan-Do-Check-Act (PDCA),* adotado pela ISO 9000.

O modelo PDCA, demonstrado na figura 2, tornou-se conhecido por identificar um método de controle de processos a fim de atingir metas preestabelecidas. É composto de quatro fases básicas: Planejamento, Execução, Verificação e Ação Corretiva. De forma sintetizada, têm-se:

- **P** (*Plan = Planejar*) - definição das metas e determinação dos métodos para alcançar as metas propostas;
- **D** (*Do = Executar*) - educação, treinamento, implementação e execução do trabalho planejado;
- **C** (*Check = Acompanhar*) - verificação contínua dos efeitos (resultados) que estão sendo obtidos no trabalho executado;
- **A** (*Act = Agir*) - atuação de correções e/ou melhorias nos processos em função dos resultados.

O modelo PDCA foi desenvolvido na década de 30 por *Shewart* tendo em *Deming* seu maior divulgador, sendo, também conhecido como *ciclo de Shewhart* ou *Ciclo de Deming* (CHIOCHETTA *et al.*, 2003).

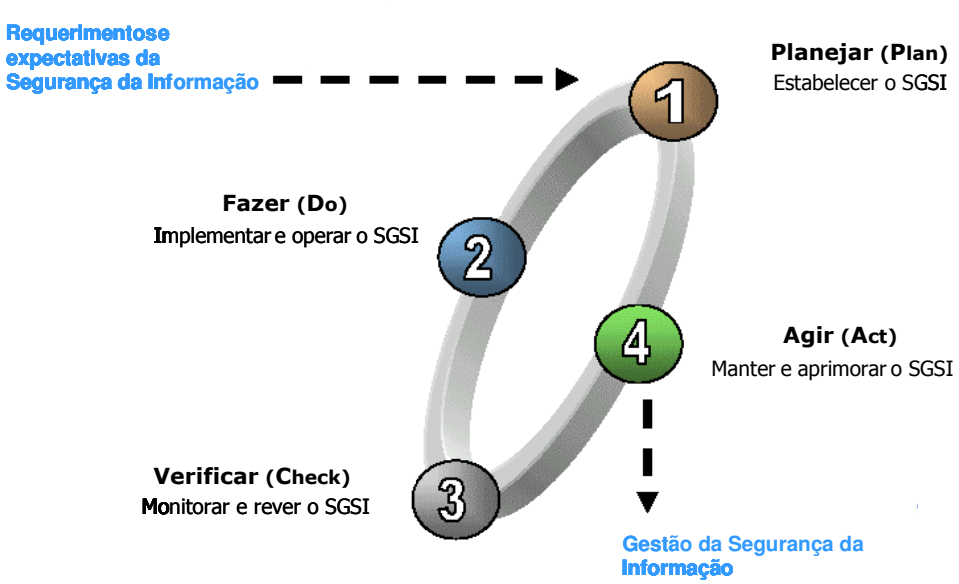

Figura 2: Estrutura do modelo de gestão PDCA aplicado ao Sistema de Gerenciamento de Segurança da Informação

Fonte: THEOBALD, John, 2003 (tradução nossa)

Além do PDI apresentado por Sêmola, outros exemplos de metodologias utilizadas para o desenvolvimento de um planejamento de atividades de segurança da informação (SI) foram identificados na revisão da literatura.

Moreira (2001), em seu livro *Segurança Mínima*, dedica um capítulo às necessidades para o planejamento de projetos de Segurança da Informação. Nesse livro, o autor aborda os requisitos necessários para a definição do escopo, equipe do projeto e identificação de necessidades das áreas de negócio que estejam relacionadas à Segurança da Informação (SI). Na abordagem de Moreira, a análise de riscos de SI, ou, na expressão do autor, "a avaliação do nível de segurança do ambiente" é o primeiro passo e balizador na definição das ações técnicas e de gestão a serem realizadas. O autor não se aprofunda, porém, a ponto de esclarecer qual o modelo proposto para a definição de prioridades, esforços e metas.

El-Gayar e Fritz (2004), propõem um modelo de suporte a decisões em segurança de sistemas de informações, denominado *multiple criteria decision making* (MCDM). A apresentação de seu modelo dá-se em forma de um processo, e é segmentado em quatro fases. Primeiro, a identificação de um problema, necessidade ou ameaça. Segundo, a análise de riscos que identifica a origem do problema. Terceiro, são geradas soluções alternativas baseadas na

criticidade percebida. Por último, é feito o planejamento de decisões baseadas na escolha da melhor alternativa entre as possibilidades identificadas.

Segundo os autores, o modelo MCDM consiste na construção de controles ou uma matriz de ameaças, e permite responder de forma simples quais controles podem ser executados para neutralizar a ocorrência de determinadas ameaças. Os autores entendem que este modelo aproveita-se ainda da possibilidade de envolver múltiplos níveis de uma organização no processo de decisão, utilizando-se de um conhecimento interdepartamental.

Já Li *et al.* (2000), apresentam a própria BS7799 como um modelo para o gerenciamento da segurança da informação, descrevendo-a como uma ferramenta capaz de auxiliar no planejamento de ações para suporte aos objetivos das organizações. Os autores apontam a BS7799 como o meio mais ágil de entendimento da segurança da informação quando se inicia um programa de gestão de SI dentro das organizações.

Em outro trabalho, Pattinson (2003) faz uma interessante combinação da metodologia *Goal Attainment Scaling* (GAS), inicialmente apresentada por Kiresuk e Lund (1982), com a linha de base dos controles de segurança extraídos da BS7799. O GAS é um método de avaliação usado para medir a efetividade de um programa ou implementação. Foi inicialmente planejado para a administração de programas sociais onde são geradas métricas para diferentes áreas. No caso do trabalho de Pattinson, a adaptação do método GAS para a segurança da informação, provê a indicação de conformidade com a norma BS7799. O autor apresenta, para tal, o exemplo de caso realizado em uma agência do governo australiano. O objetivo declarado do trabalho foi encontrar a resposta de como, usando somente a norma BS7799, as organizações poderiam medir o nível geral de segurança da informação, e ainda, estabelecer a conformidade com um padrão internacionalmente aceito. Conforme demonstrado naquele trabalho, a metodologia GAS utiliza-se de uma pontuação de cinco níveis, inseridas entre o “muito mais que o aceitável” até o “muito menos que o aceitável”, para cada controle avaliado que compõe uma matriz de nivelamento dos controles de segurança. Com o uso de uma fórmula de pontuação, os controles são agrupados de forma a facilitar a análise de atividades de SI a serem planejadas.

Para o caso apresentado, o autor realizou uma pesquisa em três etapas: a adaptação do método GAS como instrumento de avaliação do gerenciamento da segurança da informação, a utilização desta para conduzir a avaliação, e o uso dos resultados analisados para o gerenciamento. Por fim, aponta, como um de seus maiores benefícios, o envolvimento de funcionários-chaves no desenvolvimento das medidas, que fortalece a divulgação dos tópicos do método e encoraja uma melhor comunicação interna. Para Pattinson, o método GAS aplicado à segurança da informação fornece uma estrutura capaz de apontar medidas efetivas para cada controle e para suas avaliações, através de uma fórmula linear da transformação. Estas, quando combinadas com a BS7799, têm o potencial de transformar-se na base de um esquema da certificação da norma, além de gerar subsídios para uma avaliação por parte do grupo gestor da segurança.

Walton (2002) apresenta um programa realizado na Universidade de Pittsburgh para o desenvolvimento de um planejamento corporativo para a política de segurança. Chama a atenção a organização das fases e conceitos utilizados, que em muito se assemelham ao trabalho proposto neste documento. Alguns conceitos, como o de confidencialidade, integridade e disponibilidade, *Security Officer* e planejamento plurianual, são também encontrados naquele trabalho. Seu planejamento segmenta as fases de identificação dos objetivos e escopo de forma clara. Em seguida, são apuradas as disponibilidades de recursos existentes na organização e, definida uma visão futura e os produtos desejados com a implementação de programa de segurança. O autor encerra o artigo com a descrição de como deve acontecer a integração com o programa de segurança proposto das unidades de negócio e usuários-chave com as responsabilidades previstas.

O último trabalho também relevante para esta revisão foi o de Straub e Welke (1998). Os autores concentram-se, na estruturação de análise de riscos para a minimizar perdas e/ou desastres derivados de problemas de segurança de informação. Construído a partir de uma definição do planejamento de segurança da informação, o modelo de análise de riscos, segundo seus autores, se posiciona como elo de ligação entre o problema de formulação e a geração de alternativas para o planejamento da decisão. Argumentam que seu modelo

de gerenciamento de tomada de decisões é baseado em Simon (1960). Os programas de segurança propostos pelos autores incluem o uso de um modelo de análise de risco, a educação e conscientização de segurança da informação e, a formatação de um matriz de contramedidas.

As cinco fases do modelo de Straub e Welke são:

1 - O reconhecimento de problemas de segurança, onde devem ocorrer a identificação e a formulação de problemas que apresentam riscos à segurança da informação;

2 – A análise de riscos de segurança, onde se identificam as ameaças e priorizam-se os riscos;

3 – A geração de alternativas que busquem soluções para as necessidades específicas da organização, identificadas durante a análise de riscos;

4 – A etapa de decisões, onde se realiza o cruzamento de ameaças com as soluções apropriadas. É também onde ocorrem a seleção e priorização de projetos de segurança;

5 – A etapa de implementação, onde ocorre a implementação dos planos definidos na fase de decisões (fase 4), incorporando-os às soluções em andamento da organização.

2.5. Comentários finais

Apesar de sua relativa variedade e profusão, as metodologias de SI identificadas tendem a se concentrar na implementação de uma estrutura para a gestão da área de segurança da informação, sem, no entanto, esclarecer como devem ser os processos de seleção, implementação e acompanhamento das ações preventivas e corretivas aplicáveis à segurança da informação através de um sistema de gestão. Também não foram localizados trabalhos que demonstrassem como o planejamento de atividades de segurança da informação pode apoiar as necessidades de definição de prioridades, esforço, custo e utilização de recursos. Alguns autores ainda atentam à necessidade de identificação dos níveis atuais e pretendidos, sem, porém, demonstrar o

relacionamento desta identificação com os processos de negócio existentes nas organizações.

Os trabalhos analisados para esta revisão da literatura demonstram ainda haver interessantes iniciativas metodológicas para a realização de um planejamento de SI, embora ainda se perceba uma dispersão de foco e métodos. Dentre eles, o trabalho de Sêmola parece ser o único a consolidar os vários aspectos relevantes à metodologia proposta por este trabalho sem, no entanto, descrever de forma efetiva a implementação e o acompanhamento dos resultados.

Conforme descrito na tabela 2, a revisão realizada para este trabalho demonstrou haver ainda lacunas importantes na busca de uma metodologia mais aprofundada e consolidada que guie o gestor da segurança da informação no planejamento de suas iniciativas e atividades.

Autor(es)	Pontos positivos das metodologias propostas	Aspectos não contemplados e pontos negativos
El-Gayar e Fritz (2004)	• Matriz de respostas às ameaças identificadas. • Envolvimento de diversos níveis de conhecimento e comprometimento destes.	• Não identifica o nível atual e pretendido. • Indefinição de aspectos de planejamento e acompanhamento de resultados. • Ausência de embasamento em padrão comum de aceitação.
Li *et al.* (2000)	• Utilização da BS7799 como modelo para o gerenciamento de SI.	• Indefinição de aspectos de planejamento e acompanhamento de resultados.
Moreira (2001)	• Definição de escopo, equipes e necessidades.	• Ausência de estruturação para o desenvolvimento de um plano. • Não identifica o nível atual e pretendido.

Tabela 2 - Literatura analisada

Autor(es)	Pontos positivos das metodologias propostas	Aspectos não contemplados e pontos negativos
Pattinson (2003)	• Método de avaliação da efetividade de um programa implementado. • Indicação de conformidades com padrão internacionalmente aceito (BS7799). • Avalia o nível atual da gestão de SI. • Envolvimento de diversos níveis e comprometimento destes. • Método como base para a certificação com a norma BS7799.	• Indefinição de aspectos de planejamento e implementação do plano.
Sêmola (2003)	• Metodologia baseada em análises de impactos e prioridades, estudo de perímetros e estruturação de atividades. • Visão estratégica. • Direcionamento conceitual.	• Indefinição dos aspectos de implementação e acompanhamento de resultados.
Straub e Welke (1998)	• Incentiva a conscientização de SI. • Geração de matriz de contramedidas.	• Foco restrito a análise de riscos para o planejamento de decisões. • Ausência de estruturação para o desenvolvimento de um plano.
Walton (2002)	• Identificação de objetivos, escopo e recursos disponíveis. • Define visão futura e produtos. • Integração das unidades de negócio com as responsabilidades impostas pelo plano.	• Indefinição de aspectos de implementação e acompanhamento de resultados. • Ausência de embasamento em padrão comum de aceitação.

Tabela 2 - Literatura analisada (cont.)

3. MÉTODO DE PESQUISA

O objetivo deste trabalho é descrever um modelo heurístico para a implantação de um plano plurianual de segurança da informação, com base na BS7799 e na literatura disponível, onde são definidos aspectos de priorização, esforço, custeio e recursos na execução de projetos ligados à segurança da informação.

Essa pesquisa, de natureza exploratória, buscou identificar nas organizações as premissas adotadas na elaboração do planejamento de atividades de SI. Para tal, este trabalho, utilizou o conceito de modelo heurístico desenvolvido por Winter S. e adequado por Jóia em seu artigo *Um modelo heurístico para implantação de empreendimentos Government-to-Government no Brasil*. Segundo Winter (1987, *apud* Jóia, 2002, p. 3):

> "Um modelo heurístico corresponde a um grau de definição de problema que ocupa uma posição intermediária na seqüência entre uma lista longa e indiscriminada de coisas que podem importar de um lado, e um modelo teórico de controle bastante elaborado do outro. Dentro de um modelo heurístico, há espaço para uma ampla gama de formulações mais específicas do problema – mas também existe estrutura suficiente fornecida pelo próprio modelo para guiar e focalizar a discussão. Por outro lado, uma variedade rica de modelos heurísticos diferentes pode representar abordagens plausíveis para um problema apresentado".

Já, YIN (2001, p. 107), define seis fontes de evidências que permitem a realização de pesquisas qualitativas: documentação, registro em arquivos, entrevistas, observações diretas, observação participante e, artefatos físicos. Conforme, ainda, suas palavras:

> [...] "nenhuma das fontes possui uma vantagem indiscutível sobre as outras. Na verdade, as várias fontes são altamente complementares, e um bom estudo de caso utilizará o maior número possível de fontes".

Para a elaboração do modelo adequado para o desenvolvimento e implementação do de um plano plurianual de segurança de informação foi desenvolvido um modelo teórico sugerido dentre diversos que possam ser desenvolvidos num futuro próximo (Jóia, 2002, p. 2).

Adicionalmente, foram utilizados dados qualitativos obtidos através de entrevistas presenciais feitas junto a profissionais atuantes e relevantes deste mercado para avaliar a importância dada ao tema pelas suas organizações, e as principais carências percebidas pelos participantes nessa área. E, adicionalmente, uma pesquisa bibliográfica da literatura existente sobre o tema procurada nos anais da Association for Information Systems e grupos de interesse, na MISQ Central, na Association for Computing Machinery, na Asociación Española de Consultores de Seguridad Informática, e no Ibmec/RJ, além de diversos periódicos eletrônicos disponíveis na Internet, em períodos diversos compreendidos entre fevereiro de 2003 e março de 2005.

As entrevistas com os gestores de SI foram aplicadas através de um questionário semi-estruturado[5], e procuraram averiguar os principais pontos a serem contemplados num modelo para a elaboração de um Plano Diretor de Segurança da Informação (PDSI), através da identificação e avaliação das dificuldades enfrentadas, aplicabilidade, ciclo de planejamento, desenvolvimento e resultados esperados em projetos de SI em empresas brasileiras. Por se tratar de um questionário semi-estruturado, além das perguntas descritas, foram feitas questões adicionais relevantes ao contexto, conforme as circunstâncias e particularidades de cada entrevistado, sempre no intuito de averiguar a relevância de um modelo para a elaboração de um planejamento de atividades em segurança da informação.

3.1. A seleção e realização das entrevistas

Os entrevistados foram localizados através de indicações obtidas por uma lista eletrônica de alunos no mestrado do Ibmec/RJ, e de uma rede de contatos profissionais. No caso da lista eletrônica, conforme aconteciam as indicações, era feito um contato telefônico com o potencial entrevistado, onde o mesmo era informado dos objetivos e métodos da pesquisa. Com a aprovação do entrevistado, era então agendado o local, data e hora da entrevista. Conforme previsão, após o esclarecimento dos objetivos, forma e questões que seriam propostas, dos cerca de 20 potenciais entrevistados contatados, apenas seis indivíduos aceitaram participar da pesquisa. Estes, que respondem pela área de

[5] Ver – Anexo A - Questionário para entrevistas junto a *Security Officers*.

segurança da informação de empresas nos segmentos de tecnologia, telecom e serviços, realizaram entrevistas individuais, que foram gravadas e transcritas.

Cada entrevistado foi questionado se os dados que identificavam o próprio e sua organização poderiam ser divulgados. Cinco participantes solicitaram que seus dados fossem omitidos. Assim, ao longo do próximo capítulo, são utilizadas referências que não identificam os entrevistados.

3.2. Limitações da pesquisa

Por focar no desenvolvimento de um modelo para a elaboração do PDSI, este trabalho não abordou em maiores detalhes as conceituações teóricas da segurança da informação ou orientações para a estruturação da área de SI. Teve assim, como premissa, o reconhecimento da necessidade de elaboração de um planejamento de atividades de Segurança da Informação, e o entendimento por parte do leitor, das ações básicas da área de SI. Para tal, a própria BS7799:1 sugere práticas internacionalmente aceitas e a organização de um ciclo de gestão da segurança da informação.

As entrevistas utilizadas para ratificar a relevância da aplicação prática do modelo foram realizadas em apenas 6 dos 20 dos potenciais entrevistados que aceitaram fornecer informações consideradas estratégicas e sensíveis à exposição de suas empresas e, mesmo assim, sob limitações de identificação da organização a qual pertence e do próprio entrevistado. Esta situação, sugere que novos trabalhos devam ser realizados periodicamente para que se observe a movimentação dos aspectos relevantes a este estudo.

Outra observação ocorreu com as diferenças na interpretação e conceitos de segurança da informação que também poderiam afetar a elaboração do PDSI. Estas diferenças levaram à necessidade de definir um sistema de pontuação que viabilizasse a priorização dos processos a serem trabalhados. Este sistema, por sua vez, demonstrou relevante carência de referências aplicáveis à matéria.

4. ANÁLISE DOS RESULTADOS APURADOS

As informações coletadas nas entrevistas ratificaram a relevância do desenvolvimento de uma metodologia nos moldes da que será proposta neste trabalho.

A fim de tentar maximizar a aplicabilidade do modelo desenvolvido, procurou-se obter uma amostra a mais variada possível, em termos de setor e tamanho das empresas contempladas. Para tal, utilizou-se um questionário[6] semi-estruturado dividido em três partes. A primeira solicita os dados de identificação dos entrevistados e de suas organizações. Quanto à faixa etária, quase todos os entrevistados tinham entre 35 e 40 anos de idade. O tempo de atuação na área de segurança da informação estava igualmente distribuído entre as faixas 0 a 3 anos, 3 a 5 anos e, mais de 5 anos.

Quatro dos entrevistados representavam empresas da área de serviços. Um entrevistado representava uma empresa na área de tecnologia, e o outro, na área de telecom. Quanto ao porte, 4 dos entrevistados pertenciam a empresas com mais de 500 funcionários e os outros dois a empresas com números variando entre 50 e 499 funcionários.

A segunda parte da entrevista procurou enfocar a relevância dada pelas empresas aos seus departamentos/áreas de segurança da informação. Nessa parte, perguntou-se aos entrevistados qual a posição da área dentro da organização, e a quem está submetida. Cinco dos entrevistados responderam atender às diretorias ou gerências de tecnologia da informação de suas empresas, e apenas um respondeu que atende diretamente ao conselho deliberativo de sua empresa. Tais respostas sugerem que as áreas de segurança da informação, em grande maioria, ainda não atingiram uma posição hierárquica de primeiro escalão em suas empresas. Geralmente, se encontram num segundo ou terceiro nível hierárquico, sendo subalternas a uma diretoria ou gerência. Isto parece trazer limitações no provimento de orçamento, visto que a conseqüência é a subseqüente divisão dos recursos já restringidos à diretoria ou gerência a qual respondem.

---

[6] Apresentado no *anexo A* deste trabalho.

Em relação ao foco de atuação da área de SI, metade dos entrevistados respondeu ser estritamente tecnológico, enquanto a outra parte respondeu ser tanto tecnológico, quanto administrativo, atuando, também, no desenvolvimento de questões relacionadas ao posicionamento e atuação estratégica da segurança da informação, dentro da organização. Observa-se assim, uma gradual ampliação de foco destas áreas que, inicialmente, restritas a questões tecnológicas, começam a incorporar atribuições relativas à gestão política e conceitual da segurança da informação.

Todos os entrevistados disseram que suas respectivas empresas enxergam e reconhecem as áreas de SI como ponto de referência para problemas e soluções relativas à segurança da informação. Cinco dos entrevistados responderam serem convidados a discutir e opinar sobre o orçamento e estratégias nas esferas hierárquicas às quais pertencem. Ou seja, aqueles que respondem hierarquicamente à gerência ou diretoria de TI são convidados para discutir decisões em suas respectivas gerências ou diretorias. Apenas um dos entrevistados disse participar de discussões, diretamente com o conselho de sua empresa, sobre decisões estratégicas e orçamentos.

A terceira parte da entrevista, procurou identificar como os responsáveis pelas áreas de segurança de informação realizam seus planejamentos de atividades e projetos de SI. Todos os entrevistados afirmaram que realizam um planejamento de projetos de segurança. Quanto à periodicidade, cinco responderam que o fazem anualmente, e apenas um respondeu fazer um planejamento anual e trienal.

Metade dos entrevistados apontou não utilizar nenhuma metodologia específica para o planejamento, valendo-se, então, de experiências próprias. Um dos entrevistados apresentou a BS7799:1 como fonte de metodologia; outro disse se basear nas diretrizes da metodologia *Information Technology Infrastructure Library* (ITIL), e, por fim, outro ainda disse se basear em uma análise de riscos de segurança, para executar o planejamento de atividades. Na seqüência, perguntou-se como os entrevistados aplicavam tal metodologia. Para demonstrar a diversidade de iniciativas, tome-se, como exemplo, um dos entrevistados que não utiliza nenhuma metodologia específica:

> "Existem 3 *drivers* para a execução de atividades. Em primeiro lugar, o reconhecimento de necessidades [...]. O segundo é em resposta a auditorias ou trabalhos contratados que levantam demandas de segurança. E a terceira forma, [...] é reconhecimento de falhas na sua estrutura e planejar alguma ação para melhorar ou sanar estes mesmos problemas".

Todos se mostraram extremamente receptivos quanto à elaboração de uma metodologia para o planejamento de atividades de SI. Discutiu-se com todos os entrevistados os princípios e objetivos do presente trabalho, atestando sua utilidade e relevância mercadológica.

Quatro dos entrevistados disseram que utilizam apoio externo para a elaboração de seu planejamento, enquanto dois informaram utilizar somente recursos próprios para a execução do planejamento de atividades. Perguntados se os resultados obtidos até o momento eram satisfatórios, houve unanimidade na resposta que os resultados tem sido considerados positivos e eficazes. Como descrito por um entrevistado:

> "Acho que está sendo extremamente positivo, extremamente eficaz, mas não diria eficiente. Pois, embora estejamos tendo os resultados, acredito que isto poderia estar sendo numa velocidade, com uma transparência até melhor, se a gente tivesse uma maturidade maior em segurança e até em planejamento".

Em contraponto, quando questionados sobre o que poderia ser aprimorado, todos os entrevistados apresentaram sugestões. Como exemplo, o gerente de TI, Luís Castellões de Farias[7] que utilizou o modelo ITIL como metodologia para a implementação de planejamento de atividades, comentou:

> "Acho que as próprias políticas e modelos de metodologias, como o ITIL, não estão adaptados ao mercado brasileiro. Acho que as metodologias requerem uma adaptação muito rigorosa. E tem muita gente com visão acadêmica e de mercado mas pouca gente com visão prática da realidade nacional. [...] Quando você tem uma entrada de um modelo desse tipo, você tem (*mas não deveria ter, n.a.*) uma visão muito particular de um universo diferente do nosso".

Já outro entrevistado, expõe:

> "Algumas coisas iriam facilitar em muito essa evolução (dos resultados do planejamento, *n.a.*). Primeiro, um melhor entendimento pela alta direção do que

[7] Único entrevistado que permitiu sua identificação.

> é a disciplina de Segurança da Informação. Eu vejo que ainda existe um *gap* de entendimento da importância da disciplina [...]. A segunda é estruturação formal dessa área [...] com definição de papéis, limitações, missão [...] dando ciência para todos os funcionários de como funciona a área. E a terceira é a cultura, não só do usuário mas técnica das pessoas que trabalham com isso".

Estas respostas sugerem haver uma considerável variedade de iniciativas na busca de um padrão satisfatório. A ausência de referências literárias, além da falta de padronização nas iniciativas tomadas, reforçou a percepção da lacuna de referências de apoio metodológico. Embora todos tenham expressado a opinião de que os resultados obtidos até o momento são satisfatórios, também foi unânime o reconhecimento de que as iniciativas adotadas carecem de aprimoramentos, quando não, de total revisão, indicando que os resultados obtidos até o momento provavelmente não estão sendo balizados por indicadores e/ou referências de resultados.

Por fim, procurou-se saber como os entrevistados entendiam ser a percepção de suas respectivas empresas sobre os benefícios da execução do planejamento de SI. Cinco dos entrevistados disseram que os trabalhos realizados pela área são reconhecidos por suas organizações. Apenas um acredita que seus projetos passam despercebidos pela direção de sua empresa. Este, especificamente, comentou:

> "Eu acho que para a empresa isso (os benefícios gerados, *n.a.*) passa desapercebido. Até reconheço que algumas entidades reconhecem o valor e a necessidade.[...] Os benefícios da segurança são menos percebidos pelo que foi evitado, o que deixou de ser atacado ou roubado e mais pelo o que você consegue solucionar".

Disseram, ainda, haver carências, tais como um melhor entendimento da abrangência de atuação da área de SI pela alta direção, uma estruturação formal dessa área, um maior enfoque na mudança cultural das organizações, e, ainda, a adequação de uma metodologia de planejamento de segurança da informação às especificidades da empresa. O espaço corporativo para o desenvolvimento das áreas de SI parece confirmado pelo reconhecimento dos benefícios gerados pela execução do planejamento de atividades, percepção essa compartilhada pela grande maioria dos entrevistados.

Em resumo, as entrevistas realizadas indicaram haver uma lacuna acadêmica e mercadológica em função da ausência de padrão referencial de métodos e resultados aceitáveis a serem adotados pelos escritórios de segurança da informação. Outras carências identificadas como a adaptação à realidade brasileira e, a definição da composição de equipes e papéis, também foram fortemente percebidas. Tendo em vista a tendência internacional de aumento do uso de inovações exploratórias do uso da informação como um dos componentes fundamentais no novo desenho da estratégia competitiva (Borges, 1995, p. 5), o desenvolvimento da metodologia de elaboração de um plano diretor de segurança da informação, proposto neste trabalho, torna-se ainda mais relevante.

5. O DESENVOLVIMENTO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO (PDSI)

Conforme abordado na revisão da literatura, Sêmola (2003) discute os passos para a aplicação do que chama de *Solução Corporativa de Segurança da Informação*, como forma de viabilizar a aplicação de ações para maximizar retorno sobre investimentos em segurança, com a agregação de valor à organização. Como opção para a implementação de atividades de SI, Sêmola sugere a aplicação do que intitula somente de *Plano Diretor de Segurança* (PDI). Seu trabalho exerceu influência na definição das macro-etapas desta dissertação, à medida que sugere uma seqüência de ações que é coerente com a elaboração de um plano diretor de segurança da informação (PDSI). No entanto, Sêmola não explica como efetivamente o seu planejamento de segurança pode ser implementado e acompanhado. A contribuição do presente trabalho se dá justamente na formatação de um modelo heurístico que identifique os problemas, e especifique as atividades de elaboração e implementação do PDSI. Isso é feito através da aplicação de conceitos e técnicas de gestão e de SI, ilustrada por exemplos que procuram mostrar aos gestores de segurança da informação como o modelo proposto pode se adequar às necessidades diversas das organizações.

Antes de se iniciar o desenvolvimento do PDSI, é fundamental definir quem será responsável por tal iniciativa. Conforme observado nos resultados das entrevistas realizadas, o posicionamento organizacional, bem como a dedicação do gestor à área da segurança da informação (em algumas organizações, a responsabilidade sobre a segurança da informação é atribuída a um profissional responsável por uma área maior), ainda não são uniformes entre as corporações. Em linhas gerais, pode-se dizer que, quando uma empresa tem sua área de segurança da informação claramente identificada e com autonomia sobre decisões e orçamentos, deve caber ao gestor da referida área o desenvolvimento do PDSI. Por outro lado, se uma empresa interpreta a segurança da informação como atribuição adicional de outras áreas (como Tecnologia da Informação, por exemplo) é cabível a utilização de apoio de terceiros especializados no desenvolvimento do PDSI.

Tomada essa decisão, iniciar-se-á o estudo do modelo de desenvolvimento do PDSI. É sempre importante compreender que a aplicação dos passos do

modelo proposto deve ser constantemente discutido e ajustado às particularidades da estrutura, cultura organizacional, sistemas, políticas e procedimentos da organização em que se pretende aplicar o PDSI.

A seguir, serão detalhados os passos que compõem o modelo de desenvolvimento do PDSI proposto neste trabalho. Para um melhor entendimento de seu conteúdo, seus passos e conceitos serão ilustrados através do exemplo de uma empresa fictícia – a *Syllogismu S.A*.

5.1. Primeiro passo – Estudo de adequação dos controles da BS7799

É relevante que o desenvolvedor do PDSI tenha em mãos a BS7799 ou a NBR ISO/IEC 17799[8] (ISO 17799) a fim de que possa percorrer sua ordenação de controles. Com base nas particularidades estratégicas, técnicas, legais e de custos da organização, deve-se identificar quais dos 36 controles de segundo nível da referida norma são aplicáveis ao sistema de gestão da segurança da informação da organização.

Por exemplo, o controle 4.3 (*Terceirização)* lida com aspectos referentes à terceirização de serviços de segurança da informação. Supondo que, no caso da *Syllogismu*, a empresa opte por não terceirizar serviços, este controle não seria aplicável à organização. Da mesma forma, o controle 9.7 (*Monitoração do uso e acesso ao sistema)*, que descreve os aspectos relevantes à monitoração e coleta de evidências no uso dos recursos de informação, também não é aplicável, já que tal atividade é proibida por uma determinação legal regional (ABNT, 2002, p. 9 e 36).

Assim, cabe ao desenvolvedor do PDSI avaliar sempre a aplicabilidade de cada um dos 36 controles à realidade de sua organização. Por isso, a consulta da ISO 17799 é essencial, uma vez que somente o título dos controles será insuficiente para o completo entendimento de suas recomendações e prescrições.

Na tabela 3, são listados todos os controles de primeiro e segundo nível, suprimindo-se apenas os domínios 1 - *Objetivo* e 2 - *Termos e definições*, por possuírem um conteúdo apenas explicativo.

[8] Conforme esclarecido no tópico 1.4 deste trabalho, a *NBR ISO/IEC 17799* é a versão brasileira da BS7799:1, aprovada pela *Associação Brasileira de Normas Técnicas,* em agosto de 2001.

Domínio	Controles
3. Política de segurança	3.1 Política de segurança da informação
4. Segurança organizacional	4.1 Infra-estrutura da segurança da informação
	4.2 Segurança no acesso de prestadores de serviços
	4.3 Terceirização
5. Classificação e controle dos ativos de informação	5.1 Contabilização dos ativos
	5.2 Classificação da informação
6. Segurança em pessoas	6.1 Segurança na definição e nos recursos de trabalho
	6.2 Treinamento dos usuários
	6.3 Respondendo aos incidentes de segurança e ao mau funcionamento
7. Segurança física e do ambiente	7.1 Áreas de segurança
	7.2 Segurança dos equipamentos
	7.3 Controles gerais
8. Gerenciamento das operações e comunicações	8.1 Procedimentos e responsabilidades operacionais
	8.2 Planejamento e aceitação dos sistemas
	8.3 Proteção contra softwares maliciosos
	8.4 Housekeeping
	8.5 Gerenciamento da rede
	8.6 Segurança e tratamento de mídias
	8.7 Troca de informações e software
9. Controle de acesso	9.1 Requisitos do negócio para controle de acesso
	9.2 Gerenciamento de acesso do usuário
	9.3 Responsabilidade do usuário
	9.4 Controle de acesso à rede
	9.5 Controle de acesso ao sistema operacional
	9.6 Controle de acesso às aplicações
	9.7 Monitoração do uso e acesso ao sistema
	9.8 Computação móvel e trabalho remoto
10. Desenvolvimento e manutenção de sistemas	10.1 Requisitos de segurança de sistemas
	10.2 Segurança nos sistemas de aplicação
	10.3 Controles de criptografia
	10.4 Segurança de arquivos do sistema
	10.5 Segurança nos processos de desenvolvimento e suporte
11. Gestão da continuidade do negócio	11.1 Aspectos da gestão da continuidade do negócio
12. Conformidade	12.1 Conformidade com requisitos legais
	12.2 Análise crítica da política de segurança e da conformidade técnica
	12.3 Considerações quanto à auditoria de sistemas

Tabela 3: Os controles de segurança da ISO 17799 de 1º. e 2º. nível

Fonte: ABNT, 2002.

5.2. Segundo passo - Identificação do nível atual e do nível alvo de segurança

Nesta etapa, cabe ao responsável sobre a segurança da informação identificar a atual situação da organização no que tange aos aspectos de segurança da informação relacionados aos controles da ISO 17799. É nesse levantamento que se pode medir o grau de maturidade e a aderência da organização aos controles de

segurança aplicáveis, anteriormente identificados. Quando realizado periodicamente, tal levantamento permite que se acompanhe a evolução da segurança da informação de toda a organização ou de áreas específicas (TI, por exemplo). Este levantamento deve ser obtido através das observações e medidas realizadas pelo responsável pela segurança da informação. Quando aplicável, deve incluir entrevistas com gestores de áreas de negócio.

Para esta identificação é sugerida, na tabela 4, a utilização de uma escala de classificação de cinco níveis que avalia a situação atual da organização quanto aos controles aplicáveis já identificados. Essa escala de classificação inclui os seguintes níveis:

- Nível 0 – Não se aplica (N/A)

  Para controles que, por questões estratégicas, técnicas, legais ou de custos não se aplicam à organização;

- Nível 1 – Inexistente

  Controles aplicáveis, mas que não estão implementados na organização ou perímetro, e não têm previsão de implantação;

- Nível 2 – Planejado

  Controles aplicáveis ainda não implementados, mas planejados em documentação oficial da organização;

  Observação: Entenda-se por “documentação oficial da organização”, planejamentos plurianuais estratégicos, planos de metas, planos diretores de área (como o plano diretor de informática, por exemplo) ou similares.

- Nível 3 – Parcialmente implementado

  Controles em processo de implementação ou com ineficiências de operações e resultados;

- Nível 4 – Implementado/Administrado

  Controles já implementados e incorporados na organização.

Escala de Classificação	
0	Não se aplica (N/A)
1	Inexistente
2	Planejado
3	Parcialmente implementado
4	Implementado/Administrado

Tabela 4: A escala de classificação do nível de segurança

No caso da *Syllogismu*, o desenvolvedor do PDSI verificou que a empresa não utiliza nenhuma mão-de-obra terceirizada e nem tem planos de modificar esta situação. Assim, o controle 4.3 (*Terceirização)*, não é aplicável à empresa e, portanto, é classificado como nível 0 (não se aplica). Já o controle 10.3 - *Controles de criptografia*, refere-se à descrição de técnicas e sistemas criptográficos na troca de informações consideradas de risco para a corporação (ABNT, 2002, p. 9 e 40). Muito embora a *Syllogismu* não possua ainda nenhuma utilização de controles de criptografia, sua implementação está prevista no Plano Diretor de Informática, pelo qual a área de SI responde. Portanto, o controle deve ser classificado com nível 1 (inexistente).

Assim, pode-se classificar cada um dos 36 controles de 2º. nível da ISO 17799, de acordo com a escala de classificação apresentada, e conforme as situações específicas identificadas na organização.

Os resultados desse processo para a *Syllogismu*, estão dispostos na tabela 5.

Domínio	Controles	Nível	Classificação
3. Política de segurança	3.1 Política de segurança da informação	4	Implementado
4. Segurança organizacional	4.1 Infra-estrutura da segurança da informação	2	Planejado
	4.2 Segurança no acesso de prestadores de serviços	4	Implementado
	4.3 Terceirização	0	Não se aplica
5. Classificação e controle dos ativos de informação	5.1 Contabilização dos ativos	4	Implementado
	5.2 Classificação da informação	1	Inexistente
6. Segurança em pessoas	6.1 Segurança na definição e nos recursos de trabalho	4	Implementado
	6.2 Treinamento dos usuários	2	Planejado
	6.3 Respondendo aos incidentes de segurança e ao mau funcionamento	3	Parcialmente implementado
7. Segurança física e do ambiente	7.1 Áreas de segurança	4	Implementado
	7.2 Segurança dos equipamentos	4	Implementado
	7.3 Controles gerais	3	Parcialmente implementado

Tabela 5: Classificação do nível atual na *Syllogismu*

Domínio	Controles	Nível	Classificação
8. Gerenciamento das operações e comunicações	8.1 Procedimentos e responsabilidades operacionais	3	Parcialmente implementado
	8.2 Planejamento e aceitação dos sistemas	1	Inexistente
	8.3 Proteção contra softwares maliciosos	1	Inexistente
	8.4 Housekeeping	2	Planejado
	8.5 Gerenciamento da rede	3	Parcialmente implementado
	8.6 Segurança e tratamento de mídias	3	Parcialmente implementado
	8.7 Troca de informações e software	3	Parcialmente implementado
9. Controle de acesso	9.1 Requisitos do negócio para controle de acesso	1	Inexistente
	9.2 Gerenciamento de acesso do usuário	3	Parcialmente implementado
	9.3 Responsabilidade do usuário	1	Inexistente
	9.4 Controle de acesso à rede	2	Planejado
	9.5 Controle de acesso ao sistema operacional	2	Planejado
	9.6 Controle de acesso às aplicações	2	Planejado
	9.7 Monitoração do uso e acesso ao sistema	1	Inexistente
	9.8 Computação móvel e trabalho remoto	1	Inexistente
10. Desenvolvimento e manutenção de sistemas	10.1 Requisitos de segurança de sistemas	1	Inexistente
	10.2 Segurança nos sistemas de aplicação	1	Inexistente
	10.3 Controles de criptografia	1	Inexistente
	10.4 Segurança de arquivos do sistema	1	Inexistente
	10.5 Segurança nos processos de desenvolvimento e suporte	0	Não se aplica
11. Gestão da continuidade do negócio	11.1 Aspectos da gestão da continuidade do negócio	3	Parcialmente implementado
12. Conformidade	12.1 Conformidade com requisitos legais	3	Parcialmente implementado
	12.2 Análise crítica da política de segurança e da conformidade técnica	1	Inexistente
	12.3 Considerações quanto à auditoria de sistemas	1	Inexistente

Tabela 5: Classificação do nível atual na *Syllogismu* (cont.)

Uma vez pontuada a classificação dos controles de 2o. nível, é interessante consolidar os resultados obtidos a fim de possibilitar uma visualização gráfica dos mesmos. No caso da *Syllogismu*, chega-se aos seguintes dados estatísticos demonstrados na tabela 6:

Escala de Classificação		Atual	
		No.de controles	%
0	Não se aplica (N/A)	2	6%
1	Inexistente	13	36%
2	Planejado	6	17%
3	Parcialmente implementado	9	25%
4	Implementado/Administrado	6	17%
	TOTAIS	**36**	**100%**

Tabela 6: Análise da tabela de classificação do nível atual da *Syllogismu*

Os dados estatísticos podem ser representados graficamente, como demonstrado no gráfico 1. Esse gráfico poderá ser utilizado posteriormente para comparar o nível atual de segurança da organização com o nível alvo a ser atingido.

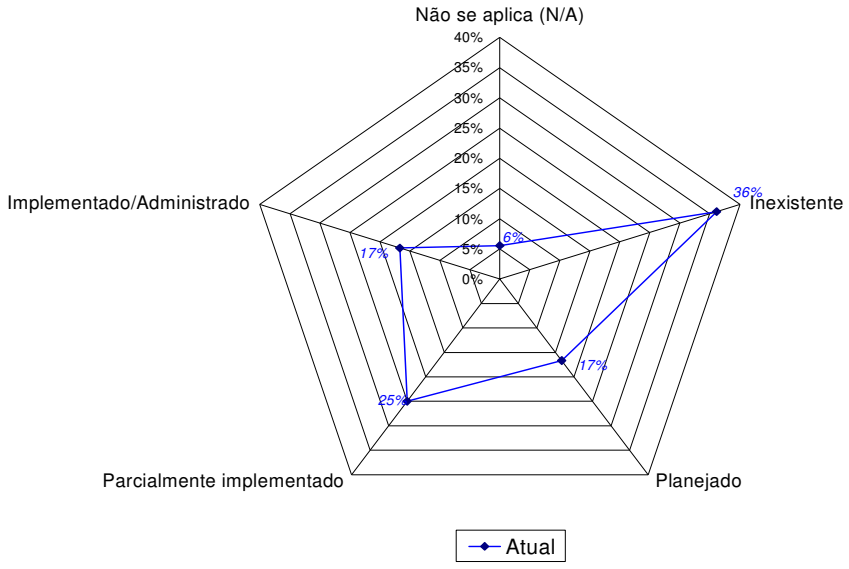

Gráfico 1: Nível atual de segurança da informação da *Syllogismu*

O resultado atingido até este momento deve espelhar o grau de amadurecimento e conscientização no tratamento dos riscos da informação. No exemplo da *Syllogismu*, os estágios *Inexistente*, *Planejado* e *Parcialmente implementado* concentram a maior parte dos controles. Isso indica um nível de maturidade baixo da empresa em relação ao tratamento dos riscos de segurança da informação.

Pode-se também visualizar os dados coletados em termos dos 10 domínios da norma NBR ISO/IEC17799. Por exemplo, para cada um deles, pode-se calcular a média dos resultados obtidos para os controles de 2º. nível do domínio. Note-se que os controles não aplicáveis não devem entrar no cálculo. Como exemplo, verifique que o domínio 6 da BS7799 – *Segurança em pessoas*,

possui três controles de 2º. nível. Estes três controles, no caso da *Syllogismu,* apresentaram, como resultados, os valores 4, 2 e 3, em suas escalas de classificação. Sua média aritmética é, portanto, igual a 3. Este resultado, juntamente com os outros obtidos na empresa, está representado no gráfico 2.

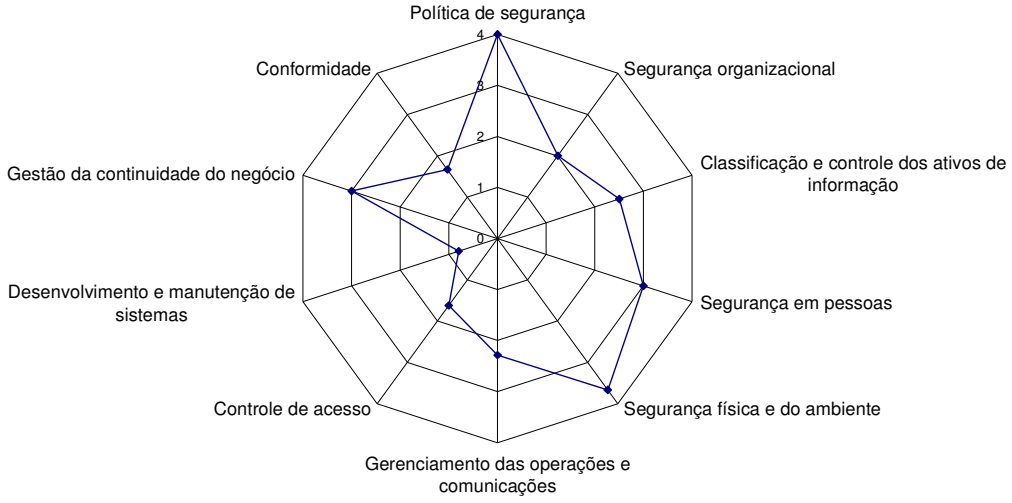

Gráfico 2: Nível atual distribuído por domínios

Este gráfico 2 destaca os pontos já fortalecidos dentro da organização, como, por exemplo, os controles relativos aos domínios de *Política de segurança* e *Segurança física e do ambiente,* bem como, domínios cujos controles apresentam clara insuficiência de resultados, como *Desenvolvimento e manutenção de sistemas*, *Controle de acesso* e, *Conformidade*.

Uma outra forma de visualização destes dados poderia ser obtida criando-se dois grupos distintos com os controles níveis 1 e 2, o outro com os níveis 3 e 4, para cada domínio. Assim, ter-se-ia uma visão mais consolidada do quão cada domínio se encontra fortalecido numa organização.

O gráfico 3, apresenta os resultados obtidos para a *Syllogismu*, utilizando esta forma de visualização.

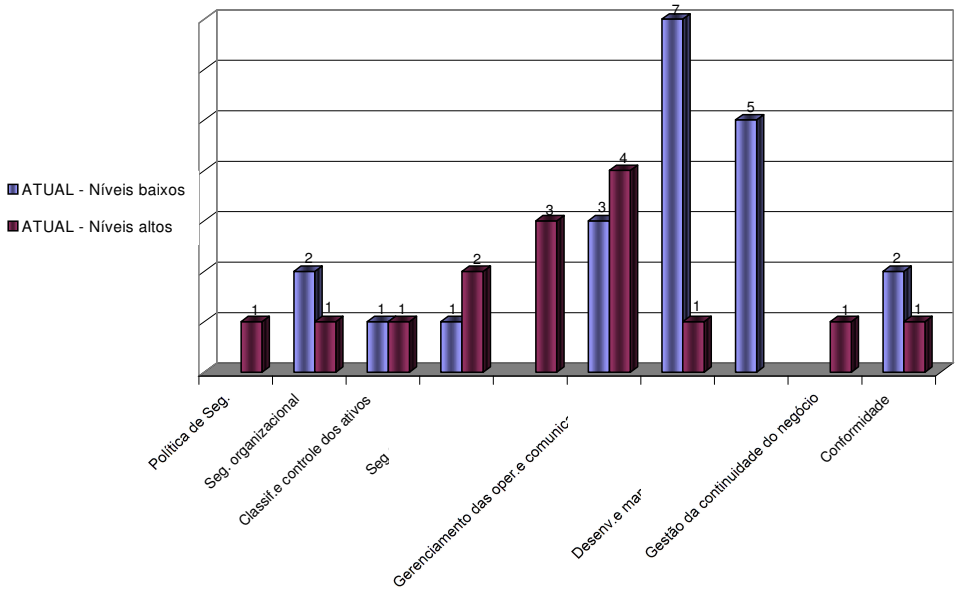

Gráfico 3: Comparação de níveis atuais baixo e alto da *Syllogismu*

Para buscar a evolução do nível geral de segurança operacional da organização, deve ser traçada uma estratégia de metas a serem atingidas com a implementação total ou parcial do PDSI. Tais objetivos devem considerar a disponibilidade de recursos físicos, financeiros, tecnológicos e humanos com que a organização possa contar, e ainda o tempo disponível para a implementação dos controles. No exemplo da *Syllogismu*, demonstrado na tabela 7, é traçado um nível alvo a ser atingido nos próximos três anos, após o início da implementação do PDSI, com verificações de evolução anual.

Domínio	**Controles**	**Nível**	**Classificação**
3. Política de segurança	3.1 Política de segurança da informação	4	Implementado
4. Segurança organizacional	4.1 Infra-estrutura da segurança da informação	3	Parcialmente implementado
	4.2 Segurança no acesso de prestadores de serviços	4	Implementado
	4.3 Terceirização	0	Não se aplica
5. Classificação e controle dos ativos de informação	5.1 Contabilização dos ativos	4	Implementado
	5.2 Classificação da informação	3	Parcialmente implementado
6. Segurança em pessoas	6.1 Segurança na definição e nos recursos de trabalho	4	Implementado
	6.2 Treinamento dos usuários	4	Implementado
	6.3 Respondendo aos incidentes de segurança e ao mau funcionamento	4	Implementado

Tabela 7: Classificação do nível alvo da *Syllogismu*

Domínio	Controles	Nível	Classificação
7. Segurança física e do ambiente	7.1 Áreas de segurança	4	Implementado
	7.2 Segurança dos equipamentos	4	Implementado
	7.3 Controles gerais	3	Parcialmente implementado
8. Gerenciamento das operações e comunicações	8.1 Procedimentos e responsabilidades operacionais	3	Parcialmente implementado
	8.2 Planejamento e aceitação dos sistemas	2	Planejado
	8.3 Proteção contra softwares maliciosos	3	Parcialmente implementado
	8.4 Housekeeping	3	Parcialmente implementado
	8.5 Gerenciamento da rede	4	Implementado
	8.6 Segurança e tratamento de mídias	3	Parcialmente implementado
	8.7 Troca de informações e software	4	Implementado
9. Controle de acesso	9.1 Requisitos do negócio para controle de acesso	2	Planejado
	9.2 Gerenciamento de acesso do usuário	4	Implementado
	9.3 Responsabilidade do usuário	2	Planejado
	9.4 Controle de acesso à rede	3	Parcialmente implementado
	9.5 Controle de acesso ao sistema operacional	3	Parcialmente implementado
	9.6 Controle de acesso às aplicações	3	Parcialmente implementado
	9.7 Monitoração do uso e acesso ao sistema	2	Planejado
	9.8 Computação móvel e trabalho remoto	3	Parcialmente implementado
10. Desenvolvimento e manutenção de sistemas	10.1 Requisitos de segurança de sistemas	2	Planejado
	10.2 Segurança nos sistemas de aplicação	2	Planejado
	10.3 Controles de criptografia	3	Parcialmente implementado
	10.4 Segurança de arquivos do sistema	2	Planejado
	10.5 Segurança nos processos de desenvolvimento e suporte	0	Não se aplica
11. Gestão da continuidade do negócio	11.1 Aspectos da gestão da continuidade do negócio	3	Parcialmente implementado
12. Conformidade	12.1 Conformidade com requisitos legais	3	Parcialmente implementado
	12.2 Análise crítica da política de segurança e da conformidade técnica	3	Parcialmente implementado
	12.3 Considerações quanto à auditoria de sistemas	2	Planejado

Tabela 7: Classificação do nível alvo da *Syllogismu* (cont.)

Para esta classificação da *Syllogismu*, controles que foram considerados não aplicáveis (nível 0) na avaliação inicial, não foram incluídos nas metas de implementação, uma vez que não se prevêem mudanças no contexto organizacional que os tornem relevantes para a empresa. Já o controle 10.3

(*Controles de criptografia)*, que tem sua implementação prevista no Plano Diretor de Informática para o próximo período e tem nível 1 (inexistente) no quadro atual, passa a ter como alvo a ser atingido o nível 3 (parcialmente implementado), com o desenvolvimento e aplicação do PDSI,

A consolidação dos alvos pretendidos para os controles de 2o. nível na *Syllogismu* resulta nos seguintes novos dados estatísticos demonstrados na tabela 8:

		Atual		Alvo	
Escala de Classificação		**Total**	**%**	**Total**	**%**
0	Não se aplica (N/A)	2	6%	2	6%
1	Inexistente	13	36%	0	0%
2	Planejado	6	17%	8	22%
3	Parcialmente implementado	9	25%	15	42%
4	Implementado/Administrado	6	17%	11	31%
	TOTAIS	**36**	**100%**	**36**	**100%**

Tabela 8: Somatório e percentual das tabelas de classificação dos níveis atual e alvo da *Syllogismu*

Diante destes novos dados é possível comparar e demonstrar graficamente os níveis atuais e alvos de segurança da informação para a *Syllogismu,* conforme demonstrado no gráfico 4.

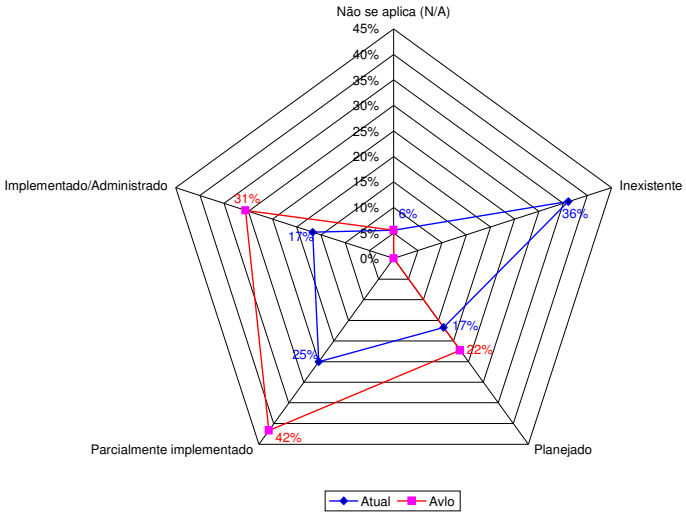

Gráfico 4: Comparação dos níveis atual e alvo da *Syllogismu*

Neste gráfico 4, se percebe um forte incremento nos estágios Parcialmente Implementado (de 25% para 42%) e *Implementado/Administrado* (de 17% para 31%), bem como a eliminação de controles no estágio Inexistente (de 36% para

0%). Estas percepções também se reproduzem no gráfico 5 onde é, novamente, demonstrada a distribuição pelos domínios de 1o. nível da norma BS7799.

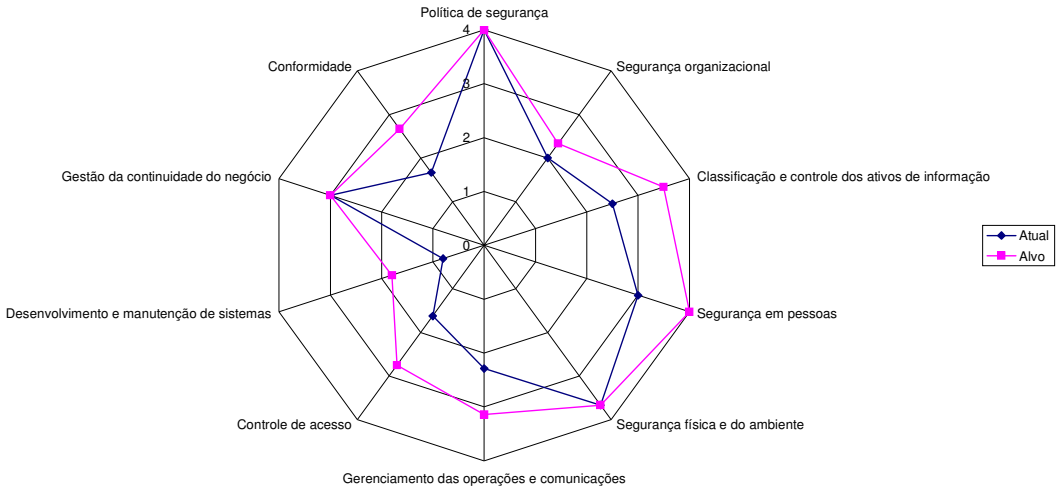

Gráfico 5: Níveis atual e alvo distribuídos por domínios

Conforme demonstrado no gráfico 6, ainda é possível comparar a terceira visualização destes dados, onde são aglutinados dois grupos com os controles de nível alvo-baixo (1 e 2) e, os de nível alvo-alto (3 e 4), por domínio.

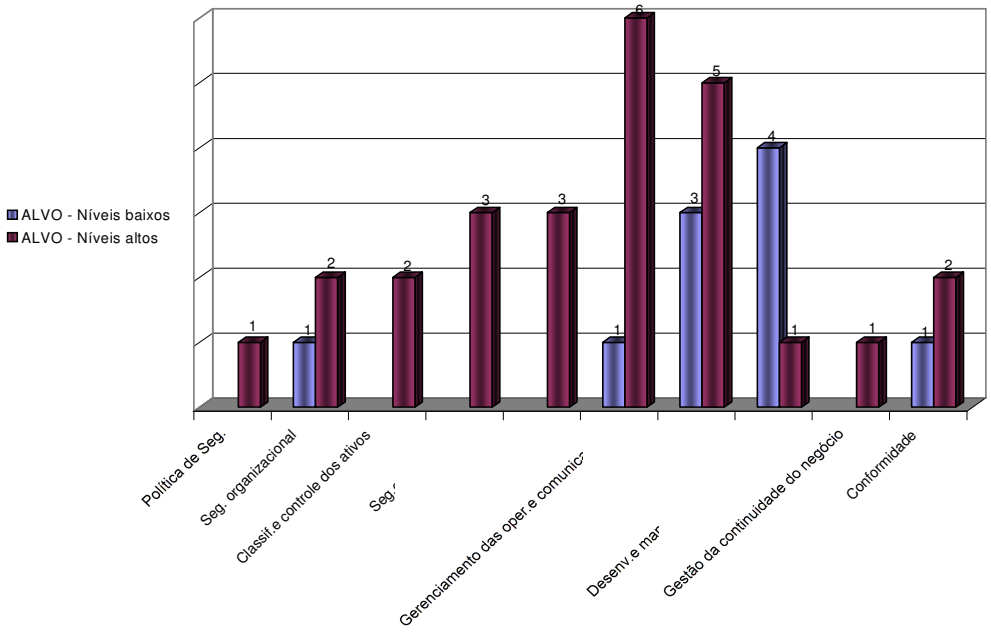

Gráfico 6: Comparação do níveis alvo - baixos e altos, da *Syllogismu*

O gráfico 6, quando comparado ao gráfico de níveis atuais (gráfico 3), mostra claramente a forte tendência de incremento nos domínios *Gerenciamento das operações e comunicações* e *Controle de acesso*. Esses movimentos

demonstram uma procura de maior nível de maturidade em relação ao tratamento dos riscos de segurança da informação, num estágio confortável de administração para a maioria dos domínios de 1o. nível, o que possibilita, inclusive, a busca da certificação BS7799 pela organização.

5.3. Terceiro passo – O levantamento dos processos de negócio

Conforme dito anteriormente, o contexto organizacional de uma empresa apresenta peculiaridades que a distinguem de outras organizações. Muito embora se encontrem semelhanças entre empresas de um mesmo ramo de atuação, a combinação de estrutura, cultura, tecnologias, processos, competências, recursos etc. são particulares em cada empresa. Para o prosseguimento da construção do PDSI, é necessário identificar o que a empresa compreende como seus principais processos de negócio.

Na definição de GONÇALVES (2000, p. 7):

> Processo é qualquer atividade ou conjunto de atividades que toma um input, adiciona valor a ele e fornece um output a um cliente específico. Os processos utilizam os recursos da organização para oferecer resultados objetivos aos seus clientes (Harrington, 1991). Mais formalmente, um processo é um grupo de atividades realizadas numa seqüência lógica com o objetivo de produzir um bem ou um serviço que tem valor para um grupo específico de clientes (Hammer e Champy, 1994).

Assim, para o desenvolvimento do PDSI, será necessário apurar junto à organização (ou eventualmente, ajudá-la a identificar) que processos de negócio são reconhecidamente críticos para aquela empresa específica, e que serão objetos do plano.

Na tabela 9, é apresentada a lista de processos e sub-processos de negócio identificados pelos gestores da *Syllogismu*.

Processos de Negócio
Financeiros
Acompanhamento de desempenho
Gestão de Caixa
Gestão de orçamento empresarial
Manufatura e comercial
Distribuição
Gestão da qualidade
Incentivos para força de vendas
Gestão de parcerias
Gestão de suprimentos
Administração geral
Desenvolvimento gerencial
Projeções econômicas e setoriais
Planejamento de recursos humanos
Planejamento de propaganda
Tecnologia da Informação
Definição de solução WEB
Gestão de serviços de rede e suporte

Tabela 9: Os processos e sub-processos de negócio da *Syllogismu*

5.4. Quarto passo – Estudo de sensibilidade (CID)

Para este quarto passo e para o quinto passo (estudo de priorização), deve-se identificar quem é ou são os executivos responsáveis pela gestão de cada processo de negócio. Uma vez identificados, é promovida uma entrevista presencial e, de preferência, individual, para evitar interferências políticas ou hierárquicas.

A entrevista deve consistir numa conversa objetiva que procure esclarecer o entendimento das operações daquele processo de negócio, utilizando exemplos de situações que resultem na quebra dos aspectos CID, para avaliar o impacto no processo.

Uma vez definidos os processos de negócio que irão compor o PDSI, sugere-se uma avaliação da sensibilidade de cada processo, em termos das propriedades básicas da segurança da informação – Confidencialidade, Integridade e, Disponibilidade (CID). No caso da *Syllogismu*, poder-se-ia supor que o processo de negócio *Gestão da qualidade* da empresa deixou vazar informações sobre uma investigação interna não concluída sobre um possível problema de qualidade de determinado lote de produtos. Esta situação caracterizaria que a confidencialidade daquele processo de negócio foi atingida sendo avaliada pelo gestor como uma evidência de quebra deste aspecto da segurança da informação.

Para fins de cadastro e organização, pode-se utilizar uma tabela auxiliar para catalogar os dados de identificação dos executivos e gestores entrevistados[9].

Para tornar as qualificações as mais objetivas possível, é sugerida a aplicação da escala, demonstrada na tabela 10, para cada um dos aspectos de segurança da informação CID:

Grau	Descrição	Significado
1	Não se aplica (N/A)	O impacto no processo de negócio (PN) é inexistente.
2	Baixo	O impacto no PN é insignificante e as respectivas atividades podem prosseguir sem conseqüências.
3	Médio	O gerenciamento do impacto é até possível, mas os prejuízos são significativos para o PN.
4	Alto	Haverá paralisação do PN. Os prejuízos serão muito significativos.
5	Crítico	Pode haver comprometimento do PN como um todo, podendo impactar outros PNs. Haverá grandes prejuízos e é difícil avaliar os custos de recuperação.

Tabela 10: Escala e significado dos níveis de sensibilidade

A tabela 11 descreve os processos de negócio e suas sensibilidades, de acordo com as entrevistas realizadas na *Syllogismu*.

Processos de Negócio	Estudo de sensibilidades		
	Confidencialidade	Integridade	Disponibilidade
Financeiro			
Acompanhamento de desempenho	4	4	3
Gestão de Caixa	4	4	4
Gestão de orçamento empresarial	3	4	4
Manufatura e comercial			
Distribuição	4	4	4
Gestão da qualidade	3	3	4
Incentivos para força de vendas	4	3	3
Gestão de parcerias	3	2	3
Gestão de suprimentos	3	3	3
Administração geral			
Desenvolvimento gerencial	3	3	3
Projeções econômicas e setoriais	4	5	5
Planejamento de recursos humanos	4	3	5
Planejamento de propaganda	4	4	3
Tecnologia da Informação			
Definição de soluções WEB	4	4	4
Gestão de serviços de rede e suporte	5	5	5

Tabela 11: Processos de negócio e estudo de sensibilidades

[9] Um exemplo desta tabela é apresentado no **Anexo C** deste trabalho.

5.5. Quinto passo – Estudo de priorização (UT)

O momento das entrevistas com os gestores dos processos de negócio pode (e deve) ser utilizado também para realizar o levantamento do estudo de priorização – Urgência e Tendência (UT). Este estudo fornece parâmetros para identificar necessidades de priorização de atividades que irão compor o PDSI.

Com este estudo realizado, é possível avaliar quais processos de negócio apresentam requisições de ações mais imediatas. Em outras palavras, deve-se ter em mente que, mesmo que um determinado processo de negócio possa ser pouco sensível a uma eventual quebra de um dos aspectos de segurança CID, o mesmo processo, com o estudo de priorização, pode ter características que necessitem de ações imediatas.

Para ilustrar a elaboração deste estudo, tome-se o processo de negócio *Gestão de parcerias* da *Syllogismu*. Assumiu-se que, por ser um processo ainda embrionário dentro da empresa, o estudo de sensibilidade CID apresentou resultados demonstram um nível razoavelmente baixo de sensibilidade à quebra de seus aspectos de segurança, conforme descrito na tabela 11. Além disso, devido a perspectivas de intensificação da execução deste processo com negócios via Web e um programa de expansão territorial da empresa, verificou-se que o estudo de priorização UT apontou para um alto nível de priorização em termos de urgência e tendência. Assim, o desenvolvedor do PDSI da *Syllogismu* deverá observar a necessidade de implementação de ações corretivas neste processo, antes dos demais.

Diferentemente do estudo de sensibilidade CID, que utilizou uma única tabela de classificação de níveis para os seus três aspectos, no estudo de priorização são utilizadas escalas de classificação específicas para Urgência e Tendência. Elas são descritas nas tabelas 12 e 13.

Urgência		
Grau	**Descrição**	**Significado**
1	Inexistente	A urgência de ação corretiva é inexistente.
2	Pode aguardar	A urgência de ação corretiva é necessária mas pode aguardar por recursos ou eventos prévios.
3	O mais cedo possível	A urgência de ação corretiva é necessária e deve ser priorizada perante as demais.
4	Imediata	A urgência de ação corretiva é imediata e devem-se utilizar todos os recursos disponíveis para tal.

Tabela 12: Escala de nivelamento – estudo de Urgência

Tendência		
Grau	**Descrição**	**Significado**
1	Estável	A tendência para o processo de negócio (PN) é de manter-se na mesma situação.
2	Deve piorar a longo prazo	A tendência para o PN é de iniciar e piorar de forma lenta mais gradual.
3	Deve piorar a curto prazo[10]	A tendência para o PN é de iniciar e piorar de forma acelerada.
4	Está piorando	O nível de vulnerabilidades de segurança do PN já está piorando.

Tabela 13: Escala de nivelamento – estudo de Tendência

Assim como no estudo de sensibilidades, será também adicionado à tabela que descreve os processos de negócio, um complemento composto pelos dados do estudo de priorização coletados nas entrevistas realizadas na empresa. Na tabela 14 é possível verificar o resultado do estudo de priorização UT da *Syllogismu*.

Processos de Negócio	Estudo de priorização	
	Urgência	Tendência
Financeiro		
Acompanhamento de desempenho	4	2
Gestão de Caixa	4	2
Gestão de orçamento empresarial	4	2
Manufatura e comercial		
Distribuição	3	2
Gestão da qualidade	3	2
Incentivos para força de vendas	3	3
Gestão de parcerias	4	4
Gestão de suprimentos	2	1
Administração geral		
Desenvolvimento gerencial	2	1
Projeções econômicas e setoriais	4	2
Planejamento de recursos humanos	3	1
Planejamento de propaganda	2	3
Tecnologia da Informação		
Definição de soluções WEB	4	4
Gestão de serviços de rede e suporte	4	4

Tabela 14: Processos de negócio e estudo de priorização UT

5.6. Sexto passo - Estudo de relevância dos processos de negócio

Com os passos realizados até o momento, o PDSI já possui os insumos fornecidos pelos gestores da organização sobre a percepção de sensibilidade e priorização de seus processos de negócio. Deve-se, no entanto, analisar tais percepções com um olhar crítico, uma vez que as mesmas foram fornecidas por

[10] Os termos “longo prazo” e “curto prazo” devem ser relativos conforme o segmento de atuação e diretrizes estratégicas da organização e do próprio processo de negócio.

seus gestores que, intencionalmente ou não, podem prover uma visão distorcida da relevância de um ou mais processos para os objetivos da organização. Assim, torna-se necessário entrevistar o executivo que possua uma visão estratégica e global da empresa, para que pontue a relevância de todos os processos de negócio para a organização. O executivo patrocinador do projeto é um potencial candidato para esta tarefa.

Para a atribuição da pontuação de relevância, pode-se utilizar uma escala de níveis, similar à utilizada no estudo de sensibilidades CID. Sua única diferença é a exclusão do nível "*Não se aplica"*, desprezado para esta segunda situação, conforme indicado na tabela 15.

Grau	Descrição	Significado
1	Baixo	A relevância do processo de negócio (PN) é insignificante para a organização, caso ocorra uma paralisação de suas atividades.
2	Médio	A paralisação de suas atividades é gerenciável, mas os prejuízos são significativos para a organização.
3	Alto	A paralisação de suas atividades trará prejuízos significativos para a organização.
4	Crítico	A paralisação de suas atividades, além do comprometimento para o PN, trará impactos aos demais. Haverá grandes prejuízos de difícil avaliação dos custos de recuperação.

Tabela 15: Escala de significado de Relevância

Deve-se perceber que este é, realmente, um momento adequado para entrevistar o executivo patrocinador e pontuar a relevância dos processos de negócio, uma vez que já se possui uma visão mais precisa dos processos da empresa e de seus gestores. Assim, o responsável pelo desenvolvimento do PDSI poderá avaliar melhor e obter esclarecimentos mais detalhados e específicos sobre as opiniões do patrocinador do PDSI.

Novamente e, como ocorrido nos estudos de sensibilidades e priorização, é adicionado à tabela que descreve os processos de negócio, os dados do estudo de relevância coletados nestas entrevistas. Conforme demonstrado na tabela 16:

Processos de Negócio	RELEVANCIA DO PN
Financeiro	
Acompanhamento de desempenho	2
Gestão de Caixa	3
Gestão de orçamento empresarial	3
Manufatura e comercial	
Distribuição	2
Gestão da qualidade	3
Incentivos para força de vendas	4
Gestão de parcerias	4
Gestão de suprimentos	1
Administração geral	
Desenvolvimento gerencial	1
Projeções econômicas e setoriais	3
Planejamento de recursos humanos	2
Planejamento de propaganda	3
Tecnologia da Informação	
Definição de soluções WEB	3
Gestão de serviços de rede e suporte	2

Tabela 16: Processos de negócio e estudo de relevância da *Syllogismu*

5.7. Estudo de perímetros tecnológicos

Em paralelo aos estudos de sensibilidade, priorização e relevância, pode-se eleger uma equipe qualificada para realizar a identificação dos perímetros tecnológicos. Esta identificação consiste em apurar, ao nível macro, os principais equipamentos de infra-estrutura tecnológica e aplicações que apóiam cada um dos processos de negócio identificados no tópico 5.3 *Terceiro passo – O levantamento dos processos de negócio*, para que sejam conhecidos os recursos que poderão sofrer ações específicas do plano. Por exemplo, o plano pode determinar que o processo de negócio *Gestão de serviços de rede e suporte* necessita de ações de segurança da informação que requeiram reconfigurações de segurança nos servidores, roteadores e aplicações que suportam o processo.

Para o estudo de perímetros tecnológicos, é sugerida a aplicação de um formulário que facilite a busca e co-relacionamento de dados capturados. A figura 3 apresenta um exemplo de sua aplicação o caso da *Syllogismu*.

Processo de negócio	**Planejamento de recursos humanos**
Sub-processo	N/A.

Levantamento feito por:	Levi Kant
Em:	16/7/2003
Observações:	N/A

Sistemas
Banco de Horas
Cadastro de pessoal
DIRF
Estrutura Orgânica
FGTS
Gestão de empregados inativos
PIS/PASEP
RAIS
Seguro
Sistema de controle aparelhos telefônicos
Sistema de controle de crachás
Sistema de controle de transporte de veículos alugados
Sistema de recisões contratuais
Sistema de treinamento à distância
Sistema gerenciador de férias
Sistema gerenciador de vale-refeição

Ativos tecnológicos
SunFire V880 - Client/Server
Sun V250 - Marte
Sun V250 - Júpiter
Firewall 1
Sun StorEdge 9980
Router - RJ01
Notes - RJ01
notes - RJ02
Sun Fire 15K - DataBase
Switch Catalyst - 6509

Figura 3: Formulário de um perímetro tecnológico de um PN da *Syllogismu*

Apenas como ferramenta de apoio visual, pode-se elaborar um diagrama do mapeamento dos principais componentes da infra-estrutura, com base nas informações apuradas sobre os equipamentos e aplicações que suportam seus

processos de negócio. A figura 4 demonstra o mapeamento de servidores e conectividade dos componentes da *Syllogismu*.

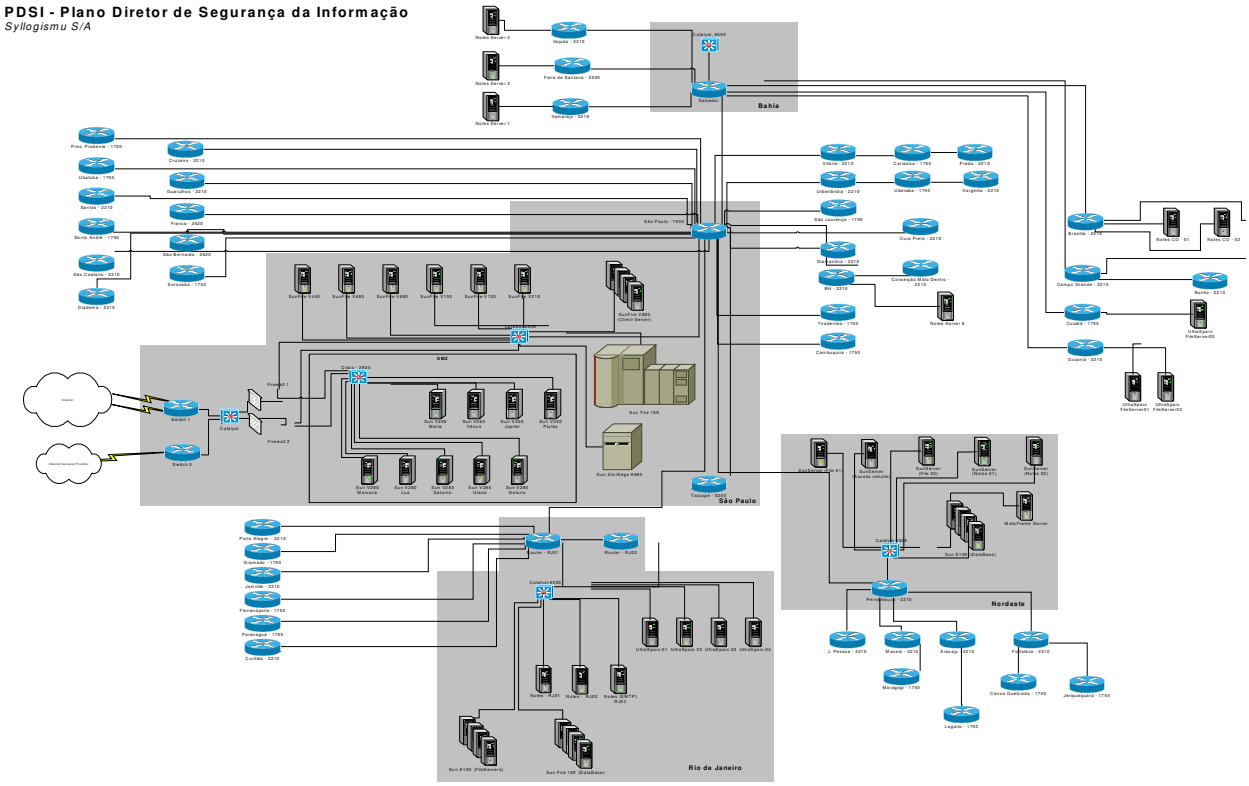

Figura 4: Mapeamento de servidores e conectividades da *Syllogismu*

5.8. Consolidação dos dados coletados

Com a execução dos passos demonstrados, fica concluída a estrutura do desenvolvimento do PDSI em suas seis etapas previstas e descritas anteriormente, conforme representado na figura 5.

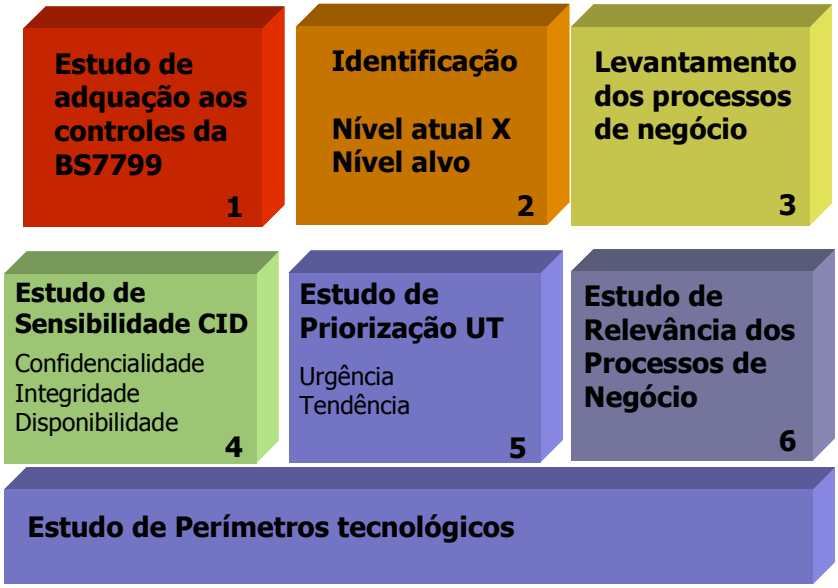

Figura 5: Estrutura de construção do PDSI

Antes de iniciar o processo de consolidação deve-se verificar se todos os documentos e formulários utilizados no levantamento de informações foram devidamente preenchidos. São eles:

- Mapa de classificação dos níveis “atual” e “alvo” da BS7799:1;
- Mapa de consolidação de estudos e relevância ;
- Mapas de perímetros dos processos de negócio ;
- Mapeamento de servidores e conectividades.

Para o caso do mapa de consolidação de estudos e relevância, as informações coletadas podem ser dispostas em uma única tabela, como demonstrado na tabela 17, para o caso da *Syllogismu*.

Processos de Negócio	Estudo de sensibilidades			Estudo de priorização		RELEVANCIA DO PN
	Confidencialidade	Integridade	Disponibilidade	Urgência	Tendência	
Financeiro						
Acompanhamento de desempenho	4	4	3	4	2	2
Gestão de Caixa	4	4	4	4	2	3
Gestão de orçamento empresarial	3	4	4	4	2	3
Manufatura e comercial						
Distribuição	4	4	4	3	2	2
Gestão da qualidade	3	3	4	3	2	3
Incentivos para força de vendas	4	3	3	3	3	4
Gestão de parcerias	3	2	3	4	4	4
Gestão de suprimentos	3	3	3	2	1	1
Administração geral						
Desenvolvimento gerencial	3	3	3	2	1	1
Projeções econômicas e setoriais	4	5	5	4	2	3
Planejamento de recursos humanos	4	3	5	3	1	2
Planejamento de propaganda	4	4	3	2	3	3
Tecnologia da Informação						
Definição de soluções WEB	4	4	4	4	4	3
Gestão de serviços de rede e suporte	5	5	5	4	4	2

Tabela 17: Mapa de consolidação de estudos e relevância da *Syllogismu*

De posse de todos os levantamentos, tem-se as informações para propor um conjunto de ações que eleve o nível de segurança da informação, definidas e priorizadas de acordo com a interpretação dos resultados obtidos nas etapas de levantamento do plano.

5.9. Determinação de um sistema de pontuação

Com a consolidação dos dados coletados, obtêm-se uma visão geral dos estudos de sensibilidade e priorização, feitos junto aos gestores dos processos de negócio, e de relevância, feitos junto ao executivo patrocinador do PDSI. Como os dados possuem diferentes origens, eles podem apresentar conflitos e distorções devido a diferenças de percepção e interpretação, que podem afetar a definição das ações do PDSI. Tais diferenças podem ocorrer em função da subjetividade inerente ao processo de avaliação, ou por questões mais objetivas, tais como a assimetria de informações.

No mapa de consolidação da *Syllogismu* disposto na tabela 17, observa-se que alguns processos de negócio tiveram um nível de criticidade à quebra dos aspectos de segurança mais alto que o definido pelo executivo patrocinador (ex.: *Gestão de Serviços de Rede e Suporte*), enquanto outros (ex.: *Incentivos para força de vendas* e *Gestão de parcerias*), parecem ser mais críticos para o executivo patrocinador do que as pontuações recolhidas por seus respectivos gestores sugerem.

Uma forma de lidar com problemas desse tipo é o uso de pesos e pontuações. Para tal, foi adaptado de TONINI em seu trabalho *Metodologia para seleção de sistemas ERP: Um estudo de caso*, a determinação de escores possíveis para os aspectos de segurança investigados e a formulação de uma equação que calcula um produto das médias geométricas dos valores obtidos nos estudos de sensibilidade e priorização, e da relevância. Para este último, deve-se negociar com alta direção da organização, o maior peso de opinião do executivo na decisão final. No modelo proposto, foi escolhido peso 2.

Deve-se atentar que a composição da equação proposta e apresentada na figura 6, é apenas uma dentre as várias possibilidades existentes e foi escolhida de forma arbitrária, o que não configura, portanto, uma regra rígida de implementação ao modelo.

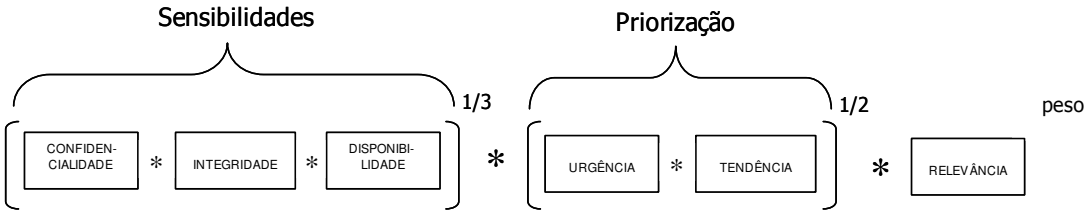

Figura 6: Equação de consolidação dos estudos

Tomando como exemplo, o processo de negócio *Acompanhamento de desempenho*, chega-se aos seguintes valores demonstrados na figura 7:

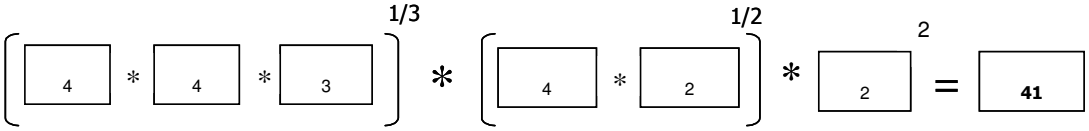

Figura 7: Equação do PN Acompanhamento de desempenho

Uma vez aplicada à equação a todos os processos de negócio da *Syllogismu*, obtém-se o seguinte resultado demonstrado na tabela 18:

Processos de Negócio	TOTAL
Acompanhamento de desempenho	41
Gestão de Caixa	102
Gestão de orçamento empresarial	93
Distribuição	39
Gestão da qualidade	73
Incentivos para força de vendas	158
Gestão de parcerias	168
Gestão de suprimentos	4
Desenvolvimento gerencial	4
Projeções econômicas e setoriais	118
Planejamento de recursos humanos	27
Planejamento de propaganda	80
Definição de soluções WEB	144
Gestão de serviços de rede e suporte	80

Tabela 18: Pontuação final dos Processos de Negócio

Com estes totais, finalmente pode-se ter uma visão dos processos de negócio da *Syllogismu* ordenados de acordo com os resultados do cálculo realizado, conforme demonstrado na tabela 19.

Processos de Negócio	TOTAL	ORDEM
Gestão de parcerias	168	1o.
Incentivos para força de vendas	158	2o.
Definição de soluções WEB	144	3o.
Projeções econômicas e setoriais	118	4o.
Gestão de Caixa	102	5o.
Gestão de orçamento empresarial	93	6o.
Planejamento de propaganda	80	7o.
Gestão de serviços de rede e suporte	80	
Gestão da qualidade	73	9o.
Acompanhamento de desempenho	41	10o.
Distribuição	39	11o.
Planejamento de recursos humanos	27	12o.
Gestão de suprimentos	4	13o.
Desenvolvimento gerencial	4	

Tabela 19: Pontuação final dos Processos de Negócio ordenada

Esses resultados permitem uma melhor interpretação dos dados coletados. Como exemplo, observe-se o processo de negócio *Gestão de serviços de rede e suporte* que teve o resultado mais alto nos estudos de sensibilidade e priorização. Este processo, devido à baixa relevância pontuada, teve sua prioridade ajustada para a sétima posição. Enquanto isso, processos como *Incentivos para força de vendas* e *Gestão de parcerias,* que obtiveram resultados baixos nos estudos de sensibilidade e priorização, graças à sua alta relevância dada pelo executivo patrocinador, apareceram na segunda e primeira posições.

5.10. O plano de ação do PDSI

A fim de atingir a evolução do nível de segurança corporativa definida na análise de identificação do nível alvo de segurança (tópico 5.2), caberá ao desenvolvedor do PDSI a elaboração de um plano de ação para a implementação dos projetos a serem propostos. Seu principal objetivo é ser um instrumento útil de orientação e priorização de atividades em função dos recursos disponíveis. No entanto, para obter o maior retorno com o menor investimento, o gestor do PDSI deve estar atento a prováveis limitações de recursos físicos, humanos, financeiros e de ordem temporal, no momento de desenvolvimento deste plano de ação.

A elaboração do plano de ação demanda talento consultivo do desenvolvedor do PDSI, pois é necessária uma grande capacidade de análise de objetivos, e visão técnica e estratégica. Ainda se espera do desenvolvedor do PDSI o conhecimento da forma de implementação e dos resultados esperados

dos diferentes serviços/projetos da segurança da informação. Ou seja, ter experiência na realização de uma análise de riscos, no desenvolvimento de uma política de segurança da informação, na implementação de controles de segurança física, em um plano de continuidade de negócios etc. Esta capacidade de entendimento propicia ao desenvolvedor do PDSI uma maior precisão no direcionamento de ações aos processos de negócio corporativos. É diante destas experiências e conhecimentos sobre os produtos de SI que o desenvolvedor do PDSI definirá a periodicidade da implementação e revisão do plano (anual, bienal etc.).

5.10.1. O processo de elaboração

O processo de elaboração do plano de ação para o PDSI inclui a montagem de um *dossiê* com todos os levantamentos, diagramas e entrevistas realizadas além de planilhas de apoio (exemplificadas nos anexos deste trabalho). Com o mapa de consolidação de estudos e relevância preenchido (anexo B), o desenvolvedor do PDSI deve dedicar minuciosa atenção aos mapas de classificação de níveis atual e alvo da BS7799:1 (Anexo E). Estes, além de serem insumos para uma visualização gráfica, têm a função de servir como direcionadores do plano de ação, pois é através deles que se devem relacionar os processos de negócio aos domínios e controles da BS7799:1. Para auxiliar na definição de prioridades, o desenvolvedor do PDSI pode entender como útil requisitar documentos complementares para a formação do *dossiê*, tais como: plano estratégico da organização (ou de TI), planejamento de novos negócios, projetos e orçamentos pré-aprovados etc. Por fim, a própria BS7799:1 deve compor este *dossiê*.

Após analisar as informações do *dossiê*, o desenvolvedor do PDSI deve iniciar a definição das atividades do plano de ação, tendo por base o mapa de conformidade dos processos de negócio com os domínios da BS7799:1 (exemplificado no anexo F). Esse mapa auxilia a visualização e montagem de uma macro-visão da aplicação de ações de segurança da informação aos processos de negócio, por domínios. Para a *Syllogismu*, seu mapa de conformidade é demonstrado na tabela 20.

Conformidade dos Processos de Negócio com os domínios da BS7799:1	Acompanhamento de desempenho	Gestão de Caixa	Gestão de orçamento empresarial	Distribuição	Gestão da qualidade	Incentivos para força de vendas	Gestão de parcerias	Gestão de suprimentos	Desenvolvimento gerencial	Planejamento de recursos humanos	Projeções econômicas e setoriais	Planejamento de propaganda	Definição de soluções WEB	Gestão de serviços de rede e suporte
0. Atividades corporativas	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3. Política de segurança	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4. Segurança organizacional									x					
5. Classificação e controle dos ativos de informação													x	x
6. Segurança em pessoas										x				
7. Segurança física e do ambiente	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8. Gerenciamento das operações e comunicações				x	x							x	x	x
9. Controle de acesso													x	x
10. Desenvolvimento e manutenção de sistemas														
11. Gestão da continuidade do negócio				x	x	x	x						x	x
12. Conformidade	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Tabela 20: Mapa de conformidade dos PNs com os domínios da BS7799:1 para a *Syllogismu*

Devem ainda compor o plano de ação, dados sobre a seqüência das etapas propostas, quais profissionais devem ser envolvidos, a área responsável pela implementação e as que serão atingidas, período de tempo de execução, esforço em horas estimado além do investimento previsto.

No mapa de conformidade da tabela 20, percebe-se a utilização de um domínio "0" denominado "Atividades corporativas". Este domínio foi inserido para que se contemplem as ações que possuem abrangência corporativa e que não se aplicam a nenhum dos demais domínios específicos da BS7799:1, como, por exemplo, uma ação de (re-)estruturação para a área de segurança da informação. Os demais domínios, foram numerados seguindo a convenção adotada na BS7799:1.

5.10.2. Atividades da segurança da informação

Como exemplo, descrevem-se a seguir algumas das atividades de SI que podem compor o plano de ação do PDSI. É importante notar que o plano de ação deve especificar as etapas e produtos finais previstos para todas as atividades que forem aplicáveis.

- Análise de Riscos de Segurança - Atividade com o propósito de mapear os riscos de segurança através da identificação dos ativos, ameaças e vulnerabilidades ;
- Implementação de controles na topologia de redes - Atividade com o propósito de analisar e especificar as necessidades de segurança através da modelagem do ambiente de redes em sua fase de planejamento ou, da reformulação de um ambiente em produção ;
- Desenvolvimento da política corporativa de segurança da informação - Atividade com o propósito de elaborar critérios para o uso de informações através do desenvolvimento de diretrizes, normas e procedimentos que orientem a sua criação ou atualização ;
- Plano de continuidade operacional de negócios - Atividade com o propósito de desenvolver estratégias e planos alternativos, que se complementam para o contingenciamento de processos, sistemas e ambientes mediante situações de quebra de disponibilidade dos serviços que atinjam as informações ;
- Treinamento em segurança da Informação - Atividade com o propósito de capacitar os empregados, parceiros e envolvidos na produção do processo de negócios sobre aspectos de gestão e proteção da segurança ;
- Campanha de conscientização dos aspectos de SI - Atividade com o propósito de sensibilizar, disseminar a cultura, comunicar os critérios e melhores práticas para o uso das informações ;
- Implementação de controles de segurança - Atividade com o propósito de viabilizar ações para corrigir falhas de segurança através da instalação e configuração de controles de caráter físico ou tecnológico.

5.10.3. Apresentação do plano de ação

São várias as estratégias de apresentação de um plano de ação. Para a formação do plano de ação do PDSI da *Syllogismu* serão descritos, para cada grupo de projetos, os seus objetivos, justificativa de recursos (humanos, físicos e financeiros) requisitados, e até três cenários de investimentos com os

respectivos períodos de execução e recursos necessários. Ao final, o desenvolvedor do PDSI pode apontar a opção de cenário de sua preferência.

Já o plano de atividades e projetos, demonstrado na tabela 21, deve demonstrar a consolidação dos projeto definidos para a organização, de forma relacionada com os domínios da BS7799:1 e com os processos de negócio aos quais os respectivos projetos irão atuar.

No exemplo a seguir, descreve-se os cenários possíveis para a processo decisório de um projeto de análise de riscos de segurança da informação para a *Syllogismu S.A.*

P2 - Análise de riscos de segurança da informação

Objetivo: Mapear a relação dos ativos e o processo de negócio, identificar ameaças e grau de vulnerabilidades, apontar os riscos e recomendar ações de correção.

Justificativa: Os desafios da gestão e redução de riscos se iniciam com o adequado mapeamento de ameaças e impactos, gerando subsídios determinantes para o adequado dimensionamento das ações corretivas que proporcionem maior retorno com menor investimento. Diante dessa certeza, o projeto se justifica com base da alta relevância para a continuidade operacional e os resultados da *Syllogismu*.

Cenário 1 – Investimento completo

Abrangência: Todos os processos de negócio

Período de execução: De M01A1 a M06A1[11]

Esforço Estimado: 1.240 horas

Competências necessárias: 1 gerente de projeto + 4 consultores de segurança
Investimento Estimado: R$93.000,00 – integral no 1º. ano do plano

Cenário 2 – Investimento moderado

Abrangência: Processos de negócio críticos e vitais

Período de execução: De M01A1 a M04A1

Esforço Estimado: 824 horas

Competências necessárias: 1 gerente de projeto + 3 consultores de segurança
Investimento Estimado: R$61.800,00 – integral no 1º. ano do plano

[11] Fica convencionada a máscara "*MxxAx*" onde, "*Mxx*" significa *Mês 01* e, "*Ax*" significa *Ano 1*.

Cenário 3 – Investimento reduzido

Abrangência: Processos de negócio vitais

Período de execução: De M01A1 a M03A1

Esforço Estimado: 618 horas

Competências necessárias: 1 gerente de projeto + 2 consultores de segurança

Investimento Estimado: R$46.350,00 – integral no 1º. ano do plano

Opção sugerida pela equipe de desenvolvimento do PDSI: Cenário 1 - Investimento completo

Para completar a apresentação do plano de ação para a implementação do PDSI, é apropriada a elaboração de um macro-cronograma, demonstrado na figura 8, para organizar os projetos propostos, de forma distribuída, ao longo de tempo de vigência, e de acordo com a percepção de prioridade de cada projeto, em função da relevância, recursos disponíveis e retorno estimado. No caso da *Syllogismu*, pode-se ver na primeira coluna do cronograma a relação que os projetos têm com os domínios da BS7799:1. As demais colunas fornecem informações de prioridade e tempo de execução dos projetos. As barras de execução dos projetos estão dispostas em duas cores, para diferenciar os projetos de abrangência corporativa dos demais projetos. Por fim, foram determinadas atividades predecessoras e sucessoras, sempre que necessárias, deixando os demais projetos livres para ajustes finos e revisões cabíveis.

5.10.4. Resultados

Como visto, o plano de ação proposto compõe-se de três principais tópicos – o plano de atividades e projetos, a descrição de cada projeto e seus cenários, e um macro-cronograma para os projetos propostos.

Assim, este capítulo descreveu os passos de elaboração e forma de implementação do plano diretor de segurança da informação, através dos domínios da BS7799:1 e definição de projetos com amplitudes específicas para os processos de negócio e de abrangência corporativa, quando aplicável. As atividades foram distribuídas e priorizadas entre os PN's mais relevantes do exemplo utilizado - a *Syllogismu,* de acordo com os levantamentos realizados. Eventuais delimitadores do plano, como orçamento e tempo de retorno, por exemplo, não foram fatores considerados na definição de projetos específicos para todos os processos de negócio da empresa.

Projeto ID	Domínio BS7799:1	Ação/Projeto	Processo de negócio
P1	0. Atividades corporativas	Reestruturação da área de segurança da informação	Todos
P2		Análise de riscos de Segurança da Informação	Todos
P3	3. Política de segurança	Desenvolvimento da Política corporativa de SI	Todos
P4	4. Segurança organizacional	Estruturação de gerenciamento do PDSI	Desenvolvimento gerencial
P5	5. Classificação e controle dos ativos de informação	Elaboração de normas de classificação da informação	Definição de soluções WEB Gestão de serviços de rede e suporte
P6	6. Segurança em pessoas	Implementação de normas e procedimentos de segurança para pessoas	Planejamento de recursos humanos
P7		Campanha de conscientização dos aspectos de SI	Planejamento de recursos humanos
P8		Treinamento em Segurança da Informação	Planejamento de recursos humanos
P9	7. Segurança física e do ambiente	Implementação de controles de segurança	Todos
P10	8. Gerenciamento das operações e comunicações	Implementação de controles na topologia de redes	Definição de soluções WEB Gestão de serviços de rede e suporte
P11		Implementação de controles para processos de operação de informação	Distribuição Gestão da qualidade Definição de soluções WEB Gestão de serviços de rede e suporte Planejamento de propaganda
P12	9. Controle de acesso	Implementação de controles de acesso físico e lógico às informações	Definição de soluções WEB Gestão de serviços de rede e suporte
	10. Desenvolvimento e manutenção de sistemas	N/A	N/A
P13	11. Gestão da continuidade do negócio	Plano de continuidade operacional de negócios	Distribuição Gestão de qualidade Incentivos para força de vendas Gestão de parcerias Definição de soluções WEB Gestão de serviços de rede e suporte
P14	12. Conformidade	Monitoramento da conformidade com a BS7799:1	Todos

Tabela 21: Plano de atividades e projetos para a *Syllogismu*

ISO	Projeto	Nome da tarefa	Início	Término	Esforço
		Plano Diretor de Segurança da Informação	**Seg 3/1/05**	**Sex 22/12/06**	7.024 hrs
0 - Atividades corporativas	P1	Reestruturação da área de Segurança da Informação	Seg 3/1/05	Seg 28/2/05	320 hrs
0 - Atividades corporativas	P2	Análise de Riscos da segurança da informação	Ter 1/2/05	Ter 6/9/05	1.240 hrs
4 - Segurança Organizacional	P4	Estruturação de gerenciamento do PDSI	Seg 3/1/05	Ter 1/2/05	168 hrs
3 - Política de Segurança	P3	Desenvolvimento da política corporativa de segurança da informação	Ter 6/9/05	Ter 7/2/06	880 hrs
5 - Classificação e Controle dos Ativos de Infor	P5	Elaboração de normas de classificação da informação	Qui 9/2/06	Qua 12/4/06	352 hrs
6 - Segurança em Pessoas	P6	Implementação de normas e procedimentos de segurança para pessoas	Ter 6/9/05	Qui 9/2/06	896 hrs
6 - Segurança em Pessoas	P7	Campanha de conscientização dos aspectos de SI	Qua 12/4/06	Sex 26/5/06	256 hrs
6 - Segurança em Pessoas	P8	Treinamento de segurança da informação	Sex 26/5/06	Seg 19/6/06	128 hrs
7 - Segurança física e do ambiente	P9	Implementação de controles de segurança	Seg 19/6/06	Sex 11/8/06	312 hrs
9 - Controle de Acesso	P12	Implementação de controles de acesso físico e lógico às informações	Sex 11/8/06	Qua 18/10/06	384 hrs
8 - Gerenciamento das Operações e Comunicaç	P10	Implementação de controles na topologia de redes	Seg 29/5/06	Sex 18/8/06	472 hrs
8 - Gerenciamento das Operações e Comunicaç	P11	Implementação de controles para processos de operação da informação	Sex 18/8/06	Sex 22/12/06	720 hrs
11 - Gestão da Continuidade do Negócio	P13	Plano de continuidade operacional de negócios	Seg 3/4/06	Sex 7/7/06	552 hrs
12 - Conformidade	P14	Monitoramento da conformidade com a BS7799:1	Seg 2/10/06	Qui 30/11/06	344 hrs

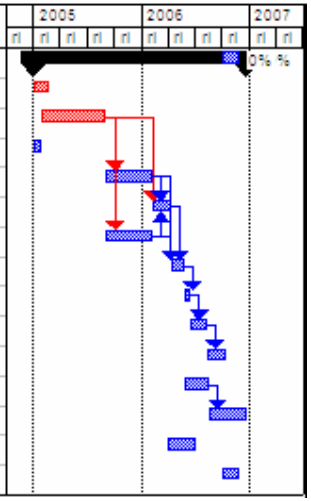

Figura 8: Macro-cronograma de atividades da *Syllogismu*

6. A IMPLEMENTAÇÃO DO PLANO DIRETOR DE SI

No plano de ação proposto para a *Syllogismu*, as descrições dos 14 projetos, demonstrados na tabela 22, devem incluir uma estimativa de utilização de recursos financeiros e profissionais para sua execução. Esta estimativa é fundamental para a defesa e embasamento do PDSI perante o nível estratégico da corporação. Com isto, além de possibilitar a programação e disponibilidade de recursos, é possível ainda ter maior domínio de alternativas para possíveis (e prováveis) reduções e/ou ajustes de escopo, tempo de execução e utilização de recursos em determinados projetos.

Deve ser, então, apresentada uma consolidação das estimativas de horas e seus respectivos custos dos projetos de acordo com os principais cenários sugeridos pelo desenvolvedor do PDSI.

Domínio BS7799:1	*Projeto ID*	Estimativa de esforço (em horas)	Estimativa de investimentos (em R$)
0. Atividades corporativas	***P1***	320	R$ 24.000,00
	P2	1.240	R$ 93.000,00
3. Política de segurança	***P3***	880	R$ 66.000,00
4. Segurança organizacional	***P4***	168	R$ 12.600,00
5. Classificação e controle dos ativos de informação	***P5***	352	R$ 26.400,00
6. Segurança em pessoas	***P6***	896	R$ 67.200,00
	P7	256	R$ 19.200,00
	P8	128	R$ 9.600,00
7. Segurança física e do ambiente	***P9***	312	R$ 23.400,00
8. Gerenciamento das operações e comunicações	***P10***	472	R$ 35.400,00
	P11	720	R$ 54.000,00
9. Controle de acesso	***P12***	384	R$ 28.800,00
11. Gestão da continuidade do negócio	***P13***	552	R$ 41.400,00
12. Conformidade	***P14***	344	R$ 25.800,00
	TOTAIS	**7.024**	**R$ 526.800,00**

Tabela 22: Estimativa de horas e custos dos projetos para a *Syllogismu*

Deve-se considerar que, em termos de gerenciamento de custos, os projetos destinados às atividades corporativas beneficiam todas as áreas de negócio da empresa. Logo, seu montante pode ser rateado por todos os processos de negócio envolvidos no PDSI. Os demais projetos devem ter seus custos divididos conforme seu impacto nos diversos processos de negócio.

Com a aprovação do PDSI pelo devidos responsáveis, será necessário o conhecimento de técnicas de gerenciamento de projetos por parte dos grupos de execução e análise de resultados do plano. É sugerido que este(s) gerente(s) de projeto venha(m) da área de segurança da informação, a fim de melhor viabilizar

o processo de implementação, através do gerenciamento de escopo, tempo e recursos dos respectivos projetos. Por último, é desejável ainda que sejam definidos indicadores de desempenho do plano, a fim de possibilitar o devido acompanhamento dos resultados obtidos, e servir de insumo para as próximas revisões do PDSI.

7. O ACOMPANHAMENTO DOS RESULTADOS – INDICADORES DE DESEMPENHO

Indicadores chaves de desempenho, ou *Key Performance Indicators* (KPI), conhecidos em algumas organizações ainda como *indicadores chaves de sucesso*, são medidas que objetivam ajudar uma organização a definir e medir seu progresso rumo aos seus objetivos organizacionais. Uma vez analisada a missão de uma organização, identificadas todas as partes interessadas e definidos seus objetivos, necessita-se de uma maneira para avaliar o progresso feito no sentido e atingir as metas especificadas o planejamento da empresa. Os indicadores chaves do desempenho executam esta função. Segundo Reh (2004, p.1, tradução nossa):

> "Os indicadores chaves do desempenho são as medidas quantificáveis, pré-acordadas e que refletem os fatores críticos do sucesso de uma organização. Estas irão diferir dependendo da organização [...]. Os indicadores chaves do desempenho são geralmente considerações de longo prazo. A definição de o que são e de como são medidas não muda freqüentemente. Os objetivos para um indicador chave de desempenho em particular podem mudar enquanto os objetivos das organizações mudam, ou enquanto começa a chegar mais perto de conseguir um de seus objetivos".

Dentro da área de segurança da informação, os indicadores chaves de desempenho devem refletir os objetivos previamente definidos para o projeto. Estes provêem à coordenação da área de Segurança da Informação os insumos para o controle dos padrões e metas estabelecidos com a implementação do plano diretor de segurança da informação, fornecendo à organização importante mecanismo de respostas quanto à adoção do plano.

8. CONCLUSÕES

A implementação de planos diretores tem se tornado uma estratégia útil e efetiva para orientar a definição de metas e objetivos corporativos. Com a crescente importância que a área de segurança da informação tem ganho nas mais diversas organizações nos últimos anos (MÓDULO, 2003, p.18), o estudo de uma metodologia para o desenvolvimento de um plano diretor, especificamente para a área de SI, já se faria justificável.

Este trabalho propôs um modelo heurístico de planejamento e implementação de um plano plurianual de segurança da informação, considerando os seus aspectos relevantes para um negócio. O planejamento proposto fornece aos desenvolvedores de um Plano Diretor de Segurança da Informação meios para identificar a situação atual e pretendida do nível de segurança da organização, a fim de tornarem-se insumos nas decisões sobre investimentos na área de segurança da informação, em conformidade com as estratégias de suas organizações.

Perante algumas lacunas observadas na revisão da literatura e nas entrevistas realizadas, este trabalho atendeu as necessidades de referência para um modelo de planejamento e implementação de projetos de segurança da informação, fornecendo meios de definir visões de maturidade sobre os conceitos de segurança em conformidade com padrões internacionalmente aceitos.

Em relação à sua aplicabilidade, o modelo proposto não se restringe a nenhum segmento de atuação específico sendo aplicável a diversos segmentos do mercado brasileiro. Como diz Jóia (2002, p. 3):

> "Um modelo é bom não por causa do excesso de rigor que aplica a si mesmo, medido pelo número de variáveis levadas em consideração, mas sim pelo fato de modelar e expressar adequadamente a realidade que se enfrenta".

Deve-se alertar que, embora alguns dos princípios da metodologia já tenham sido aplicados em organizações reais, é importante avaliar os resultados e dificuldades encontradas em implantações do modelo por completo.

Considerando-se que o imaturo entendimento dos aspectos e conceitos da segurança da informação ainda varia entre as organizações, tem-se ainda um campo fortemente carente de aprofundamento em sua pesquisa científica e operacional.

Indiferentemente de quaisquer fatores, as propostas apresentadas devem ser compreendidas como regras maleáveis, tendo em vista a diversidade de ramos de atuação, culturas organizacionais e tendências mercadológicas. Assim, reforça-se o entendimento que o trabalho aponta estratégias e métodos aplicáveis a diferentes áreas de atuação sem, com isso, ter a pretensão de especificar regras rígidas de implementação à realidade das organizações.

BIBLIOGRAFIA

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: ABNT, 2002.

BARBOSA, Paulo. **Security Office**, 2002. Atualizada em: 13 abr. 2004. Acesso em: 27 abr. 2004. Disponível em <http://www.theprime.com.br/research/artigos/artigo_secoffice.htm>.

BASTOS, Alberto. **Os novos rumos da gestão de segurança com as normas ISO 17799 e BS7799,** 2002. Atualizada em: 2 mai. 2003. Acesso em: 2 mai. 2003. Disponível em <http://www.modulo.com.br/index.jsp>.

BORGES, Mônica Erichsen Nassif. **A informação como recurso gerencial das organizações na sociedade do conhecimento**. Revista Ciência da Informação, v. 24, n. 2, p. 5, 1995.

BROERSMA, Matthew. **Estudo revela que companhias gastam pouco com segurança** - revista eletrônica COMPUTERWORLD, 2004. Atualizada em: 15 set. 2004. Acesso em: 27 set. 2004. Disponível em <http://computerworld.uol.com.br/AdPortalV3/adCmsDocumentoShow.aspx?Documento=27934>.

CASANAS, Alex Delgado Gonçalves e, MACHADO, César de Souza. **O impacto da implementação da norma NBR ISO/IEC 17799 – Código de prática para a gestão da segurança da informação – nas empresas**, 2003. Atualizada em: 3 ago. 2004. Acesso em: 18 ago. 2004. Disponível em <http://egov.alentejodigital.pt/Page10549/Seguranca/iso17799-1.pdf>.

CHIOCHETTA, João Carlos; KOVALESKI, João Luiz; BOARETTO, Neury; e, SANZONVO, Nadia. **Processos de Gestão: Descomplicando a questão da qualidade**. Revista Eletrônica de Ciência Administrativa, Ed. 4, 2003. Atualizada em: 28 out. 2003. Acesso em: 14 de junho de 2004. Disponível em <http://www.presidentekennedy.br/recadm/edicao4/artigo10.pdf>.

COMPUTERWORLD, Revista eletrônica. **Web tem sete vezes mais vírus que ano passado**. 2004. Atualizada em: 28 nov. 2004. Acesso em: 30 nov. 2004. Disponível em <http://computerworld.uol.com.br/AdPortalV3/adCmsDocumentoShow.aspx?documento=29490&Area=1>.

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

EL-GAYAR, Omar F.; FRITZ, Brian D. **A framework for decision support in information systems security**. Proceedings of the tenth Americas Conference on Information Systems. Nova Iorque, Agosto 2004.

ERNST & YOUNG, **Global Information Security Survey**, 2002. Atualizada em: 2 abr. 2003. Acesso em: 7 jan. 2005. Disponível em <http://www.ey.com/GLOBAL/ccr.nsf/Images/5A554029E120389B85256CFC004E22A7/$FILE/GIS2002.pdf>.

FARAH, Moisés Francisco Jr. **Reestruturação produtiva e estratégias de gestão: o caso de uma média empresa do setor metalúrgico da região metropolitana de Curitiba**. Curitiba, 1999.

GLOBO ONLINE, Revista eletrônica. **Volume de informação dobrou em três anos.** 2003. Atualizado em 04 nov. 2003. Acesso em: 04 nov. 2003. Disponível em **<**http://arquivoglobo.globo.com**>.**

GOMES, Wagner. GLOBO ONLINE, Revista eletrônica. **Bancos lideram investimento em inovação tecnológica**. 2005. Atualizado em 16 mar. 2005. Acesso em 16 mar. 2005. Disponível em <http://arquivoglobo.globo.com>.

GONÇALVES, José Ernesto Lima. **As empresas são grandes coleções de processos**. RAE – Revista de Administração de Empresas, v.40, n.1 p. 7, jan/mar 2000.

HAMMER, Michael; CHAMPY, James. **Reengineering the corporation**. New York: HarperBusiness, 1994.

HARRINGTON, H. James. **Business process improvement**. New York: McGraw Hill, 1991.

HOLLANDA, Aurélio Buarque de. **Novo Aurélio Século XXI: o Dicionário da Língua Portuguesa**. 3. ed. Rio de Janeiro: Nova Fronteira, 1999.

IDG NOW!, Revista eletrônica. **Vírus geram 87% dos problemas de segurança**. 2004. Atualizada em: 2 jun. 2004. Acesso em: 14 dez. 2004. Disponível em <http://idgnow.uol.com.br/AdPortalv5/SegurancaInterna.aspx?GUID=B1AFD87A-BE91-4951-89F1-D008CFF5B98D&ChannelID=21080105>.

INTERNET SECURITY GLOSSARY, **Request for Comments 2828**, 2000. Atualizada em: 25 ago. 2004. Acesso em: 8 fev. 2005. Disponível em <http://www.faqs.org/rfcs/rfc2828.html>.

ISMS International User Group. **International Register of BS7799 Accredited Certificate**, 2004. Atualizada em: 31 mar. 2005. Acesso em: 8 abr. 2005. Disponível em <http://www.xisec.com/register.htm>.

JOIA, Luiz Antonio. Um modelo heurístico para implantação de empreendimentos Government-to-Government no Brasil. In: VII Congresso Internacional Del CLAD sobre la Reforma Del Estado y de la Administratción Pública. Lisboa, out. 2002.

KIRESUK, T.J.; LUND, S. H. **Goal Attainment Scaling: A medical-correctional application**. Medicine and Law, Vol. 1, pp. 227-251, 1982.

LEAL, Pedro Flores. **Tendencias en la administración del capital intellectual**, 1998. Atualizada em: 8 set. 1998. Acesso em: 27 mar. 2003. Disponível em <http://www-csc.mty.itesm.mx/cgi-bin/csc/HN_sc116_abr99/get/sc116_abr99/13.html>.

LI, Haiwen; KING, Graham; ROSS, Margaret; STAPLES, Geoff. **BS7799: A Suitable Model for Information Security Management**, 2000. Atualizada em: 25 mai. 2001. Acesso em: 7 set. 2003. Disponível em <http://aisel.isworld.org/Publications/AMCIS/2000/042.pdf>.

MARINHO, Zilta Penna. **Security Officer – quem é esse profissional e quais suas funções?**, 2003. Atualizada em: 13 out. 2003. Acesso em: 13 out. 2003. Disponível em <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=213&pagecounter=0&idiom=0>.

MÓDULO SECURITY SOLUTIONS, **9ª. Pesquisa Nacional de Segurança da Informação**, 2003. Atualizada em: 24 nov. 2003. Acesso em: 3 dez. 2004. Disponível em <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>.

MOREIRA, Nilton Stringasci. **Segurança mínima**. Rio de Janeiro: Axcel Books, 2001.

PATTINSON, Malcolm R. **Compliance with an Information Security Management Standard: A New Approach**, 2003. Atualizada em: Acesso em: 4

jul. 2003. Acesso em: 17 mai. 2005. Disponível em <http://aisel.isworld.org/Publications/AMCIS/2003/03GA06.pdf>.

POWER, Richard. **CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends**, 2002. Atualizada em: 20 jun. 2002. Acesso em: 29 dez. 2004. Disponível em <http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Survey.pdf>.

REH, F. John. **Key Performance Indicators**, 2004. Atualizada em: 5 jan. 2005. Acesso em: 5 jan. 2005. Disponível em <http://management.about.com/cs/generalmanagement/a/keyperfindic.htm>.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – uma visão executiva**. Rio de Janeiro: Campus, 2003.

SIMON, H**. The new science of management decision.** New York: Harper and Brothers, 1960.

STRAUB, Detmar W.; WELKE, Richard J. **Coping with systems risk: security planning models for management decision making**. Atlanta: MIS Quarterly, vol. 22, pp. 441-469, 1998.

THEOBALD, John. **The Road to BS7799 Accreditation and using ISO 17799 as an Information Security Framework**, 2003. Atualizada em: 2 mar. 2003. Acesso em: 18 nov. 2004. Disponível em <http://www.itsecurity.com/papers/idefence1.htm>.

TONINI, Antonio Carlos. **Metodologia para estabelecimento de critérios de seleção de um sistema ERP**. In: CONGRESSO DE CUSTOS, 9. Fecap, São Paulo, ou. 2002.

WALTON, Jinx P. **Devoloping and enterprise information security policy**, Pittsburgh, 2002. Atualizada em: 5 dez. 2002. Acesso em: 3 set. 2004. Disponível em <http://delivery.acm.org/10.1145/590000/588678/p153-walton.pdf?key1=588678&key2=6760668011&coll=GUIDE&dl=ACM&CFID=38929572&CFTOKEN=92082763>.

WINTER S. (1998). **Knowledge and Competence as Strategic Assets**, In: The Strategic Management of Intellectual Capital, Klein D. (ed.), pp. 165-187, Butterworth-Heinemann.

YIN, Robert K. **Estudo de Caso: planejamento e Métodos**. 2º. ed. Porto Alegre: Bookman, 2001.

Anexo A - Questionário para entrevistas junto a Security Officers

1 - Dados de identificação:

a) Nome:

b) Empresa:

c) Qual a sua função na empresa:

2 - A empresa:

a) Onde se encontra a área responsável pela segurança das informações dentro da organização? E a quem esta área responde hierarquicamente?

b) Qual o foco do *Security Office* na empresa?

c) A área possui o reconhecimento da empresa como referencial nas decisões na área de segurança da informação?

d) O *Security Officer* é convidado a participar das decisões estratégicas da organização?

3 - Planejamento de atividades/projetos

a) O *Security Office* faz um planejamento plurianual do orçamento a ser investido em projetos? Qual a sua periodicidade?

b) É utilizada alguma metodologia para a execução deste planejamento? Qual?

c) Como se aplica esta metodologia?

d) O *Security Office* contrata alguma consultoria externa para este planejamento?

e) Os resultados obtidos até o momento são satisfatórios?

f) O que deve ser aprimorado?

g) Qual a percepção da empresa dos benefícios gerados pela execução deste planejamento?

Anexo B – Mapa de consolidação de estudos e relevância

Processos de Negócio	Estudo de sensibilidades			Estudo de priorização			RELEVÂNCIA DO PN
	Confidencialidade	Integridade	Disponibilidade	Gravidade	Urgência	Tendência	

Anexo C - Catálogo de identificação de entrevistados

Empresa:	
Local:	
Cidade/UF:	

Relevância

Executivo:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Estudo de sensibilidades e prioridades

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Gestor:		**Entrevista**	
Departamento:		*Data:*	
Email:		*Hora:*	
Telefone:		*Local:*	

Anexo D – Mapa de perímetros do processo de negócio

Processo de negócio	
Sub-processo	

Levantamento feito por:	
Em:	
Observações:	

Sistemas

Ativos tecnológicos

Anexo E – Mapa de classificação de níveis da BS7799:1

Domínio	Controles	Nível	Classificação
3. Política de segurança	3.1 Política de segurança da informação		
4. Segurança organizacional	4.1 Infra-estrutura da segurança da informação		
	4.2 Segurança no acesso de prestadores de serviços		
	4.3 Terceirização		
5. Classificação e controle dos ativos de informação	5.1 Contabilização dos ativos		
	5.2 Classificação da informação		
6. Segurança em pessoas	6.1 Segurança na definição e nos recursos de trabalho		
	6.2 Treinamento dos usuários		
	6.3 Respondendo aos incidentes de segurança e ao mau funcionamento		
7. Segurança física e do ambiente	7.1 Áreas de segurança		
	7.2 Segurança dos equipamentos		
	7.3 Controles gerais		
8. Gerenciamento das operações e comunicações	8.1 Procedimentos e responsabilidades operacionais		
	8.2 Planejamento e aceitação dos sistemas		
	8.3 Proteção contra softwares maliciosos		
	8.4 Housekeeping		
	8.5 Gerenciamento da rede		
	8.6 Segurança e tratamento de mídias		
	8.7 Troca de informações e software		
9. Controle de acesso	9.1 Requisitos do negócio para controle de acesso		
	9.2 Gerenciamento de acesso do usuário		
	9.3 Responsabilidade do usuário		
	9.4 Controle de acesso à rede		
	9.5 Controle de acesso ao sistema operacional		
	9.6 Controle de acesso às aplicações		
	9.7 Monitoração do uso e acesso ao sistema		
	9.8 Computação móvel e trabalho remoto		
10. Desenvolvimento e manutenção de sistemas	10.1 Requisitos de segurança de sistemas		
	10.2 Segurança nos sistemas de aplicação		
	10.3 Controles de criptografia		
	10.4 Segurança de arquivos do sistema		
	10.5 Segurança nos processos de desenvolvimento e suporte		
11. Gestão da continuidade do negócio	11.1 Aspectos da gestão da continuidade do negócio		
12. Conformidade	12.1 Conformidade com requisitos legais		
	12.2 Análise crítica da política de segurança e da conformidade técnica		
	12.3 Considerações quanto à auditoria de sistemas		

Anexo F – Mapa de conformidade dos processos de negócio com os domínios da BS7799:1

Conformidade dos Processos de Negócio com os domínios da BS7799:1	Processo de negócio I	Processo de negócio II	Processo de negócio III	Processo de negócio IV	Processo de negócio V	Processo de negócio VI	Processo de negócio VII	Processo de negócio VIII	Processo de negócio IX	Processo de negócio X
0. Atividades corporativas										
3. Política de segurança										
4. Segurança organizacional										
5. Classificação e controle dos ativos de informação										
6. Segurança em pessoas										
7. Segurança física e do ambiente										
8. Gerenciamento das operações e comunicações										
9. Controle de acesso										
10. Desenvolvimento e manutenção de sistemas										
11. Gestão da continuidade do negócio										
12. Conformidade										

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo